The Massachusetts
Department of Public Health
'Helping People Lead Healthy Lives In Healthy Communities'

Massachusetts Department of Public Health Confidentiality Policy and Procedures

Effective May 3, 2004

MDPH Privacy Office
250 Washington St.
Boston, MA 02108

Massachusetts Department of Public Health
Confidentiality Policy and Procedures

Table of Contents

Massachusetts Department of Public Health
Confidentiality Policy and Procedures

MDPH Confidentiality Policy

Introduction

To further its mission, the Massachusetts Department of Public Health (the "Department") collects confidential information for use in public health surveillance, program development and evaluation, research, and for many other public health purposes. The Department also collects information from individuals seeking certain services or benefits. It is critical that Department workforce members recognize the importance of protecting personal privacy and safeguarding the confidentiality of information obtained by the Department to the greatest extent possible.

Each citizen of the Commonwealth has a fundamental right to privacy and confidentiality with respect to any confidential information held by the Department. Individuals have rights related to how information about them is collected, used, maintained, and disclosed. Individually identifiable information must be treated confidentially, and individuals should be given easily understood information about policies regarding the collection, use, maintenance, and disclosure of confidential information. Individuals' authorization for the disclosure of their identifiable confidential information should be obtained for anticipated disclosures, unless disclosure of these data without authorization is required or allowed by law or regulation.

Individuals' claims to privacy must be balanced with their public responsibility to contribute to the common good, through use of their information for important public health purposes, with the understanding that their information will be used with respect and be protected as required by law. For instance, health information is vital to public health surveillance, public health investigations, collection of vital records, and research studies about the population's health. Health information is essential to the Department's performance of basic public health activities, and the protection of confidential information about individuals is an important responsibility of the Department. Thus, the Department strives to balance its mission to protect the health and safety of the public with its commitment to safeguarding the privacy rights of its citizens.

This Confidentiality Policy is intended to ensure that Department workforce members comply with all relevant state and federal laws and regulations concerning the protection of confidential information. These include, but are not limited to, the Massachusetts Fair Information Practices Act (FIPA); the Health Insurance Portability and Accountability Act (HIPAA) and the privacy and security regulations implementing HIPAA, as they apply to the Department as a hybrid agency;[1] and Massachusetts Executive Order # 412. Other

[1] Hybrid Entity means MDPH as a single legal entity, whose business activities include both covered and non-covered functions and that designates the covered functions to be included in its covered components. Only covered components are required to comply with HIPAA's Privacy and Security Rules. All covered and non-covered components must follow the Department's Confidentiality Policy and Procedures, except where otherwise indicated.

specific state and federal laws and regulations may impose additional confidentiality requirements. Examples include state laws regarding HIV/AIDS, cancer incidence information, and vital records and federal laws regarding confidentiality of substance abuse and Women, Infants and Children (WIC) nutrition program information. This Confidentiality Policy applies to all Department workforce members in the covered and non-covered components of the Department and establishes the general rules that all Department workforce members are expected to follow concerning use and disclosure of confidential information collected and maintained by the Department. The specific procedures that must be implemented by each Center in the Department are contained in the confidentiality procedures.

Limiting Collection of Confidential Information

Department workforce members shall collect confidential information only when such collection is authorized by law or regulation, when confidential information is deemed necessary to further a public health purpose, or when provided to the Department by individuals seeking services or benefits. Workforce members shall collect no more confidential information than is reasonably necessary to accomplish the intended purpose.

Limiting Use of Confidential Information

Department workforce members shall limit the use of confidential information to those purposes for which the information was collected or other public health purposes permitted by law, which further the mission of the Department. Whenever identifiable information is not necessary to conduct the public health purpose, the confidential information shall be rendered de-identified.

Limiting Access to Confidential Information

Department workforce members shall limit access to confidential information to only those workforce members who have a legitimate need to access the information in order to conduct the public health purpose. Access shall be limited to the minimum number of individuals who are reasonably necessary to conduct the public health purpose.

Limiting Disclosure of Confidential Information

Department workforce members shall limit disclosure of confidential information to only authorized persons. Department workforce members shall follow the confidentiality procedures, which delineate when and to whom disclosures can be made. Department workforce members shall limit disclosure of confidential information to the minimum necessary amount of confidential information that is required to accomplish the intended purpose of the use or disclosure.

Acknowledgment of Confidentiality Policy and Procedures

All Department workforce members shall strictly maintain the confidentiality of all confidential information held by the Department. No person having access to confidential information shall disclose, in any manner, any confidential information except as established in the confidentiality procedures. All Department workforce members will receive education and training regarding the confidentiality and security principles addressed in this policy and the procedures. In addition, all Department workforce members shall sign an acknowledgement that they received training and that it is their responsibility to read and comply with all aspects of the Confidentiality Policy and Procedures.

Data Linkage

If confidential information is used for data linkage, the linked dataset shall be stripped of personal identifiers and all identifiers shall be destroyed unless there is a legitimate public health purpose for retaining such identifiers. When such projects involve individuals who are not Department workforce members, Department workforce members shall conduct data linkage projects in-house whenever possible and disclose only the linked dataset without personal identifiers, other than a unique identification number, unless otherwise approved by the Commissioner.

Data Destruction

As soon as reasonably practicable and in a manner consistent with Commonwealth record retention policies, Department staff shall de-identify confidential information and destroy all identifiable information unless there is a legitimate public health purpose for retaining such identifiable information or retention of the information is required by law. Limited data sets that are used or disclosed must be destroyed or returned to the primary data holder when projects for which they were obtained are completed.

Publications and Reports Based on Confidential Information

All reports and publications based on confidential information shall contain only aggregate data. No personally identifiable information or information that could lead to the identification of an individual shall be published or disclosed, unless pursuant to an authorization. All aggregate data presented in such reports or publications shall comply with Department procedures on aggregate data release to ensure that individuals cannot be identified based on the data presented. No maps based on confidential information may be published or disclosed with sufficient detail so as to allow for identification of individuals.

Individual Rights

The Department is committed to providing individual data subjects with access to confidential information held by the Department, unless otherwise restricted. The Department shall take appropriate measures to permit individual data subjects to amend or to restrict the disclosure of their confidential information subject to certain restrictions. An opportunity to request specific individual rights related to confidential information held by the Department shall be afforded to all data subjects. All workforce members shall follow procedures that provide for these rights.

Security

Department workforce members who have access to confidential information shall ensure that such information is maintained in a secure manner which prevents unauthorized individuals from gaining access to such information. Confidential information shall not be removed from the work site unless authorized as necessary for work related purposes, shall not be transmitted by email unless by means of a Departmental approved secure system, and shall not be downloaded to a portable device unless authorized by the Center director. Workforce members shall follow all applicable procedures to ensure physical and electronic security of all confidential information. Department workforce members shall not attempt to exceed the scope of their authorized access or attempt to circumvent any Department systems security measures.

Data Integrity

The Department will work to ensure the quality, accuracy, and reliability of the data and records under its control, whether contained in written, electronic, or other format. The Department will only collect confidential information that is relevant to the purposes for which it is to be used, and will work to ensure that such data is accurate, complete, and timely. Department workforce members must ensure that confidential information is protected from unauthorized modification and destruction. The Department shall strive to maintain the accuracy of the confidential information it holds. This includes establishing, where appropriate, mechanisms to allow individuals access to review and amend their confidential information if permitted by and in compliance with state and federal law.

Research Studies and Contact with Data Subjects

Department workforce members that are conducting a research project, which requires access to confidential information held by the Department, shall consult with the Research and Data Access Review Committee (RaDAR) and the Office of the General Counsel to ensure that appropriate research protocols are followed and that review by the Human Research Review Committee (HRRC) at Shattuck Hospital (i.e., the Department's Institutional Review Board) is obtained when necessary. In addition,

Department workforce members that are conducting a research study or other public health investigation, which involves contact with data subjects, shall consult with the Office of the General Counsel to review and approve the contact protocol (consent forms, questionnaires, interview scripts, etc.).

Confidential Information Procedures

Each Center of the Department shall implement the specific procedures adopted pursuant to this policy. A Center may adopt additional procedures that specifically address the operations of the Center provided that the procedures are consistent with this policy and are reviewed and approved by the Privacy Office. Department workforce members shall comply with all procedures adopted pursuant to this policy.

Compulsory Legal Process and Requests from Law Enforcement

Any Department workforce member receiving a subpoena, discovery request, court order or any other form of compulsory legal process to provide confidential information shall immediately notify the Office of the General Counsel (OGC) and shall not disclose any confidential information until authorized to do so by the Office of the General Counsel, unless the Center and the OGC have a protocol that does not require contacting the OGC. Any workforce member receiving a request for access to confidential information from a law enforcement official shall immediately notify the Office of the General Counsel or the Privacy Office and shall not disclose any confidential information unless and until authorized to disclose the information.

Non-Compliance

All Department workforce members are required to comply with the Confidentiality Policy and Procedures. Department workforce members that fail to comply may be denied further access to confidential information and may be subject to disciplinary action. Department workforce members shall immediately report to their Privacy Office any violations of this policy. Department workforce members are protected from retaliation for reporting violations of the Confidentiality Policy and Procedures by Massachusetts law (M.G.L. c. 149, §185). The Department may audit use and disclosure of confidential information by Department workforce members in order to ensure compliance with this policy and the procedures. The Confidentiality Policy and Procedures continue to apply to workforce members after leaving MDPH, with respect to confidential information to which the workforce member had access while working at the Department.

CONTACT INFORMATION

Any questions concerning this policy should be directed to the Privacy Office at:

MDPH Privacy Office
Massachusetts Department of Public Health
250 Washington Street
Boston, MA 02108
(617) 624-6083

Questions relating to any of the MDPH Hospitals or the State Office of Pharmacy Services should be directed to their respective Privacy Office:

Lemuel Shattuck Hospital: (617) 971-3550
Massachusetts Hospital School: (781) 830-8877
Tewksbury Hospital: (978) 851-7321, ext. 2211
Western Massachusetts Hospital: (413) 562-4131, ext. 232
Office of State Pharmacy Services: (978) 858-2100

Effective Date: May 3, 2004

Confidentiality Policy and Procedures Glossary

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

For the purposes of the Department's Confidentiality Policy and Procedures, the following words and phrases shall have the following meanings:

Access means the provision by the Department to an individual of an opportunity to inspect or review confidential information about that individual held by the Department.

Acknowledgment means a written statement, dated and signed by all workforce members, that certifies the individual's agreement to abide by the Department's Confidentiality Policy and Procedures.

Aggregate Data means data collected from individual-level records that have been combined for statistical or analytical purposes and that are maintained in a form that does not permit the identification of individuals.

Authorization means the permission that a data subject or his or her personal representative gives to another person or entity allowing that person or entity to disclose the data subject's confidential information.

Business Associate (BA) means a person or entity who, on behalf of a covered component of the Department, and other than in the capacity of a workforce member, performs or assists in the performance of a function or activity that involves the use or disclosure of confidential health information; or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services, where the provision of the service involves the use or disclosure of confidential health information.

Cell Size Suppression means a statistical method used to report aggregate data in tables that restricts or suppresses disclosure of subsets of aggregate data to protect the identity and privacy of data subjects and to avoid the risk of identification of individuals in small population groups.

Confidential Information means, unless otherwise defined by law, any individually identifiable information, including, but not limited to, medical and demographic information, that:

1. Reveals the identity of the data subject or is readily identified with the data subject, such as name, address, telephone number, social security number, health identification number, or date of birth; or
2. Provides a reasonable basis to believe that the information could be used, either alone or in combination with other information, to identify a data subject.

Confidential Information includes any protected health information, as defined by HIPAA, and any personal data, as defined by FIPA. To the extent that certain information held by the Registry of Vital records is deemed under state law to be unrestricted, this information is not confidential information for the purposes of these procedures. Nothing in the Confidentiality Policy or Procedures shall be read or interpreted to restrict the disclosure of Registry information, where identifiable information is otherwise unrestricted and permitted to be disclosed.

Confidentiality means the Department's obligation to protect the health and other personal information with which it is entrusted.

Consent means voluntary agreement with what is being done or proposed (express or implied).

Contact means to communicate or attempt to communicate with a data subject or the data subject's parent, guardian, or health care provider by any means, including, but not limited to, in-person, telephone, facsimile, letter, or electronic mail.

Covered Health Care Component means those programs that would meet the definition of a covered entity if each were a separate legal entity. It may also include a program:

1. To the extent that it performs a covered function, but does not strictly meet the definition of a covered entity (i.e., a provider that does not transmit information electronically in connection with a covered transaction); or
2. It engages in activities that would make it a business associate of a component that performs covered functions if the two were separate legal entities.

Covered Entity (CE) means a health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form relating to any covered transaction.

Custodian means the program or bureau that holds and maintains the data that is shared pursuant to an Intra-Department Data Use Agreement with another program or bureau in the Department.

Data Holder has the same meaning as under FIPA, and means an agency which collects, uses, maintains or disseminates personal data or any person or entity which contracts or has an arrangement with an agency whereby it holds personal data as part of as a result of performing a governmental or public function or purpose.

Data Linkage means a method of assembling data contained in two or more different files or records to relate significant health and other events for the same individual, organization, community, or other unit of analysis.

Data Subject means the individual about whom the data or information relate.

De-Identified Data means information that has been subject to methods for rendering it not individually identifiable, such as the removal of personal identifiers including, but not limited to, name, address, telephone number, social security number, health identification number, or all elements of dates except year relating to the individual.

Disclosure means the transfer, dissemination, release, or communication by other means of any confidential information to any person or entity outside the Department or for a HIPAA covered component, outside the covered component.

Electronic Confidential Information means information defined as confidential information in this glossary, which is stored or transmitted by electronic media.

Electronic media means:

1. *Electronic storage media* including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
2. *Transmission media* used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Faxes sent directly from one fax machine to another, person-to-person telephone calls, video teleconferencing, and messages left on voice-mail are not considered transmission media. However, any faxes sent from a computer, including those made by a fax-back system, are considered transmission media.

Fair Information Practices Act (FIPA) means M.G.L. c. 66A, the state law protecting the confidentiality of personal data held by state agencies or entities conducting business on behalf of state agencies.

Health Information has the same meaning as under the HIPAA Privacy Regulation, and means any information, whether oral or recorded in any form or medium, that:

1. Is created or received by the Department; and
2. Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Health Insurance Portability and Accountability Act (HIPAA) means the federal law passed in 1966 that was intended to reform the health insurance market and simplify the health care administrative processes. While the HIPAA legislation addresses many issues, the provisions that directly effect the Department of Public Health are contained in Title II, Subtitle F - Administrative Simplification and the regulations relating to Privacy, Security and Transactions and Code Sets, implemented pursuant to the Administrative Simplification requirements.

Hybrid Entity means MDPH as a single legal entity under HIPAA, whose business activities include both covered and non-covered functions, and that designates the covered functions to be included in its covered components. Only covered components are required to comply with HIPAA's Privacy and Security regulations. All covered and non-covered components must follow the Department's Confidentiality Policy and Procedures, except where otherwise indicated.

Indirect Treatment Relationship means a relationship between an individual and a health care provider in which:

1. The health care provider delivers health care to the individual based on the orders of another health care provider; and
2. The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the service or products or reports to the individual.

Individual means the person who is the subject of confidential information.

Individual-Level Data means any data or information collected and maintained concerning a specific individual.

Individually Identifiable Health Information has the same meaning as under the HIPAA Privacy Regulation, and means information that is a subset of health information, including demographic information collected from an individual, and:

1. Is created or received by the Department; and
2. Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Institutional Review Board means any board, committee, or other group formally designated by an institution, and approved by the federal Department of Health and Human Services pursuant to 45 C.F.R. Part 46 to review, approve, and periodically evaluate research projects to protect the rights of human research subjects.

Limited Data Set means, as described in Procedure 7, confidential information that excludes specific direct identifiers of the individual, or of relatives, employers or household members of the individual, which may be disclosed for public health or operations purposes, at the discretion of the Department, provided that a Limited Data Set Use Agreement is executed. A comparable data set may be disclosed for research purposes, if approved by the Department's RaDAR committee and an agreement is executed.

Personal Data has the same meaning as under FIPA, and means any information concerning an individual which, because of name, identifying number, mark or description can be readily associated with a particular individual, provided that such information is not contained in a public record.

Personal Representative means a person authorized under state law to act on behalf of an individual (data subject). Certain information may be collected from or disclosures may be made to personal representatives if they are so authorized under Massachusetts law.

Pledge of Confidentiality means a written statement, dated and signed by an individual who is granted access to confidential information that certifies the individual's agreement to abide by the confidentiality restrictions stated in the written statement.

Privacy means the right of an individual to control the disclosure of data or information about himself or herself, freedom from unreasonable interference in an individual's private life, and an individual's right to protection against inappropriate disclosure of his or her personal data.

Protected Health Information has the same meaning as under the HIPAA Privacy Regulation, and means individually identifiable health information, with limited exceptions, that is:

1. Transmitted by electronic media;
2. Maintained in any medium described in the definition of electronic media in the Privacy Regulation; or
3. Is transmitted or maintained in any other form or medium.

Protected Health Information is a subset of Confidential Information.

Public Health Authority has the same meaning as under the HIPAA Privacy Regulation, and means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Public Health Purpose means a population-based activity primarily aimed at the reduction of morbidity or mortality; the prevention of injury, illness, disease, disability or premature mortality; the improvement of health outcomes; or the promotion of health in the community, including assessing the health needs and status of the community through public health reporting and surveillance, developing public health policy, and responding to public health needs and emergencies.

Public Record has the same meaning as under the Massachusetts Public Records Law, M.G.L. c. 4, § 7(26), and means all books, papers, maps, photographs, recorded tapes, financial statements, statistical tabulations, or other documentary materials or data, regardless of physical form or characteristics, made or received by an officer or employee of any agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or of any political subdivisions thereof, or of any authority established by the general court to serve a public purpose, unless such materials or data fall within the listed exemptions.

Required By Law means, with respect to confidential information, a mandate contained in law that compels an entity to make a use or disclosure of confidential information and that is enforceable in a court of law. Required by law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Research means a systematic investigation designed primarily to develop or contribute to general knowledge, including public health, medical, social, demographic and historical research.

Safe Harbor Method means, as defined in as under the HIPAA Privacy Regulation and Procedure 7, that data are deemed to be de-identified when all specified identifiers are removed.

Security means the manner of assessing the threats and risks posed to data and taking the appropriate steps to protect that data against unintended or unauthorized access, use, intrusion, or such other dangers as accidental loss or destruction.

Subpoena means a formal request to compel the Department to produce an individual to testify or to produce documents in relation to a proceeding in which the Department may or may not be a party to the action. A subpoena may be issued by an attorney or, in some instances, by the court. It is often accompanied by a witness fee. Failure to respond to a subpoena may result in legal sanctions.

Surveillance means the public health function of monitoring the occurrence and spread of disease and indications of such occurrence and spread.

Treatment, Payment and Health Care Operations (TPO) has the same meaning as under the HIPAA Privacy Regulation and includes the following:

- Treatment means the provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care.

- Payment means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collections activities, medical necessity determinations and utilization review.
- Health Care Operations includes functions such as quality assessment and improvement activities, reviewing competence or qualifications of health care professionals, conducting or arranging for medical review, legal services and auditing functions, business planning and development, and general business and administrative activities.

Use has the same meaning as under the HIPAA Privacy Regulation, and means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information among the non-covered components and within each covered component.

Workforce Members means all employees, volunteers, interns, long-term temporary workers, trainees, and other persons whose conduct, in the performance of work for the Department is under the direct control of the Department, whether or not they are paid by the Department.

Procedure Title:	Administrative Requirements		
Procedure Number:	1	**Version #**	2.0
Effective Date:	May 3, 2004		

Content

I. Purpose and Scope

This procedure describes the Department's obligations related to the implementation of the Confidentiality Policy and Procedures. While the Confidentiality Policy and Procedures will be implemented generally through the Department's Centers, in certain instances it may be more appropriate to implement procedures at the Bureau or program level. This procedure applies to both covered and non-covered components of the Department, and all workforce members.

II. Personnel Designations

The Department must designate and document the following:

A. Privacy Officer

The Department must designate an individual to be the Privacy Officer for the Department. The Privacy Officer is responsible for the development and implementation of the Department's Confidentiality Policy and Procedures. Each MDPH Hospital shall also designate a Privacy Officer.

B. Privacy Liaisons[2]

Each Center and certain Bureaus shall designate a contact person to serve as a liaison to the Privacy Office. The privacy liaisons will work with the Privacy Office to help Centers and Bureaus meet and monitor compliance with the requirements of

[2] Information related to the Department's privacy liaisons is available at http://healthnet/privsec/linfo.htm.

the Confidentiality Policy and Procedures. Privacy liaisons will also work with the Privacy Officer in resolving any complaints related to privacy and confidentiality as required in Procedure # 13: Complaints Regarding the Use and Disclosure of Confidential Information.

C. Security Officer

The Department must designate an individual to be the Security Officer for the Department prior to the April 21, 2005 compliance date for the HIPAA Security Rule. The Security Officer is responsible for the development and implementation of Department-wide policies and procedures relating to the security of confidential information.

III. Privacy and Confidentiality Training Requirements

The Department must meet the following obligations related to training workforce members:

- **A.** Each new and returning workforce member shall receive training on their responsibilities under the Confidentiality Policy and Procedures within a reasonable time after starting work at the Department;[3]
- **B.** Each workforce member whose functions are affected by a material change in the Confidentiality Policy and Procedures, or by a change in position or job description, must receive training within a reasonable time after the change becomes effective;
- **C.** Workforce members who routinely have access to confidential information will receive additional confidentiality training as it relates to specific job functions; and
- **D.** The Department must document and maintain records of the successful completion of privacy and confidentiality training by workforce members.

IV. Safeguards for Confidential Information

Each Center must comply with the administrative, technical, and physical safeguards described in Procedure # 10: Security Of Confidential Information to protect against intentional or unintentional, unauthorized uses or disclosures. In addition, Department programs that are designated covered health care components under the Department's hybrid entity status[4] must have safeguards in place to protect against unauthorized disclosures of confidential information to non-covered components within the Department.

[3] The Department's current privacy and confidentiality training requirements can be found at http://healthnet/privsec/training.htm.

[4] More information related to the Department's hybrid entity status under HIPAA can be found at http://www.state.ma.us/dph/comm/hipaa/dphhipaa.htm.

V. Complaint Process

A. All complaints regarding the Department's obligations and compliance with the Confidentiality Policy and Procedures should be directed to the MDPH Privacy Office. The Privacy Office will consult with the appropriate privacy liaison to investigate the complaint as described in Procedure # 13: Complaints Regarding the Use and Disclosure of Confidential Information.

B. All complaints regarding the MDPH Hospitals' obligations and compliance with their confidentiality procedures should be directed to their respective designated privacy contacts. The hospital receiving the complaint shall initiate the investigation of the complaint, and upon completion of the investigation file a report with the Department's Privacy Office.

VI. Sanctions

As described in Procedure # 2: Sanctions for Breaches of Confidentiality, the Department will enforce sanctions against workforce members who fail to comply with the Department's Confidentiality Policy and Procedures.

VII. Mitigation

A. Each Center must mitigate, to the extent feasible, any harmful effects from unauthorized uses or disclosures of confidential information by any member of the Department's workforce.

B. If any workforce member discovers that confidential information was disclosed in error, a written report must be timely completed and forwarded to the workforce member's supervisor or Center's privacy liaison or the MDPH Hospital's designated privacy contact, who shall provide a copy to the MDPH Privacy Office. The report shall include a description of what occurred, including to whom the disclosure was intended, who received the confidential information, and what was done to mitigate any harmful effects of the disclosure.

C. Mitigation may include, but is not limited to, contacting the erroneous recipient and requesting that the information be returned, destroyed and/or deleted. Supervisors shall also evaluate necessary steps to preclude future erroneous disclosures, including retraining the responsible workforce member, or restricting the member's access to confidential information.

D. Determination of any additional steps required to mitigate the effects of the disclosure will be accomplished through consultation with the appropriate Center Director, the Privacy Officer and the Office of the General Counsel.

VIII. Retaliation Prohibited

No member of the Department's workforce shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising his or her rights under the Confidentiality Policy and Procedures, or for participation in

any process relating to compliance with the Policy and Procedures. Workforce members are protected from retaliation for reporting violations of the policy and procedures in accordance with M.G.L. c. 149, §185.

IX. Required Policy and Procedures

The Department must document the following actions relating to the Confidentiality Policy and Procedures:

A. Policy and Procedures

The Department shall implement a Confidentiality Policy and Procedures to ensure the privacy and security of confidential information. A Center or Bureau may adopt additional procedures that specifically address its operations, provided that the procedures are consistent with Department's Policy and Procedures, and they are available for review by the Privacy Office.

B. Changes to Policies and Procedures

The Department must revise its policy and procedures whenever necessary to conform to changes in law or regulation. The Department may also revise its policy and procedures at any time when deemed necessary to meet the needs of the Department. The Privacy Officer will provide notice to Center and Bureau Directors and privacy liaisons whenever the Confidentiality Policy or Procedures are revised.

C. Documentation Requirements

The Department must maintain current and prior versions of the required policy and procedures in written or electronic form, and any other written documentation relating to the policy and procedures, for a period of six years from the date of creation, or as required by the Records Conservation Board.[5]

X. Employee Acknowledgement

All current Department workforce members[6], and new workforce members at the time of hire shall sign a Confidentiality Acknowledgement agreeing to abide by the Department's Confidentiality Policy and Procedures. Copies of signed Confidentiality Acknowledgements shall be maintained permanently by the Human Resources Department (HRD). For workforce members that are not captured by HRD, the Bureau Director or Supervisor shall maintain the acknowledgement. Contractors and agents of the Department that will have access to confidential information must sign a confidentiality pledge or other acceptable confidentiality agreement, as approved by the Privacy Officer. Department workforce members shall agree to protect confidential

[5] Information related to the Massachusetts Records Conservation Board is available at http://www.state.ma.us/sec/arc/arcrcb/rcbidx.htm.

[6] This requirement does not apply to workforce members engaged for a period of time less than one month.

information from unauthorized disclosure even after termination of employment or other contractual obligations.

Authority: M.G.L. c. 66A, §§ 2(a) and (b)
45 C.F.R. § 164.530

Forms: Confidentiality Acknowledgment

Procedure Title:	Sanctions for Breaches of Confidentiality		
Procedure Number:	2	**Version #**	2.0
Effective Date:	May 3, 2004		

Content

I. Purpose and Scope

This procedure specifies the sanctions and possible disciplinary actions that may result from violation of the Department's Confidentiality Policy and Procedures, or applicable state or federal law. This procedure applies to both covered and non-covered components of the Department and all Department workforce members.

MDPH is strongly committed to ensuring that workforce members perform their duties in a professional manner that protects the confidentiality of sensitive information. However, nothing in this procedure should be construed to contain binding terms and conditions of employment or to constitute a contract between MDPH and its workforce members.

II. Disciplinary Sanctions

Any workforce member who breaches confidentiality in violation of the MDPH Confidentiality Policy and Procedures is subject to discipline up to and including termination of employment. Disciplinary actions will be handled in accordance with applicable laws, collective bargaining agreements, civil service regulations and MDPH procedures depending on the type of workforce member being disciplined. Generally, the type of sanction will depend on the intent of the individual and the severity of the violation. The offenses listed below, while not all-inclusive, are organized according to the severity of the violation.

A. Group I: Improper and/or Unintentional Disclosure of Confidential Information or Records

This level of breach occurs when an individual workforce member unintentionally or carelessly accesses, reviews or reveals confidential information to him or herself or others without a legitimate need-to-know. Examples include, but are not limited to: individuals discuss confidential information in a public area; an individual leaves a copy of client confidential information in a public area; an individual leaves a computer unattended in an accessible area with confidential information unsecured.

B. Group II: Unauthorized Use and/or Misuse of Confidential Information or Records

This level of breach occurs when a workforce member intentionally accesses or discloses confidential information in a manner that is inconsistent with the MDPH policy and procedures, but for reasons unrelated to personal gain. Examples include, but are not limited to: an individual looks up information related to a friend or relative; an individual reviews the record of a client/patient out of curiosity or concern.

C. Group III: Willful and/or Intentional Disclosure of Confidential Information or Records

This level of breach occurs when a workforce member accesses, reviews or discloses confidential information for personal gain or with malicious intent. Examples include, but are not limited to: an individual accesses information to sell to a private business; an individual accesses personal information and uses it for harassment or to spread gossip.

III. Other Sanctions

Workforce members who violate state or federal law for the improper use or disclosure of confidential information may be subject to criminal investigation and prosecution or civil monetary penalties.

IV. Documentation

A. Initial Reporting

Workforce members who are aware of a breach of confidentiality must immediately report it to their supervisor. Failure to report a breach, of which one has knowledge, will result in appropriate disciplinary action. Reporting of a breach in bad faith or for malicious reasons will result in appropriate disciplinary action.

B. Filing Requirements

Supervisors must document any disciplinary actions taken against an employee in the employee's personnel file. Supervisors must also make the MDPH Privacy Officer aware of any improper uses or disclosures so that appropriate mitigation

measures may be taken. The Privacy Officer will review willful or intentional breaches of privacy to determine if such incidents should be reported to the appropriate state or federal authorities.

Authority: M.G.L. c. 66A, § 2(b)
45 C.F.R. § 164.530(e)

Procedure Title:	Use and Disclosure of Confidential Information		
Procedure Number:	3	**Version #**	2.0
Effective Date:	May 3, 2004		

Content

I. Purpose and Scope

This procedure describes:

- The limited circumstances when Centers may collect, use, and disclose confidential information.
- The Department's *minimum necessary standard*, which requires Centers to limit the amount of confidential information they collect, use and disclose to only the information necessary for the intended purpose; and
- The Department's *role-based access standard*, which requires Centers to ensure that access to confidential information, is limited to appropriate workforce members.

This procedure applies to both covered and non-covered components of the Department, and all Department workforce members.

II. Collection of Confidential Information

A. When Confidential Information May be Collected

Confidential information may only be collected when:

1. Required or authorized by law or regulation;
2. Authorized by the data subject based on a valid authorization as specified in Procedure # 4: Authorizations for the Use and Disclosure of Confidential Information;
3. Submitted by the data subject when obtaining services or benefits offered or funded by the Department;[7]
4. Submitted to the Department for research purposes pursuant to M.G.L. c. 111, § 24A. The Department's requirements related to research are described in Procedure # 6: Research Requirements; or
5. Submitted by a vendor pursuant to a contract with the Department.

B. Procedures for Handling Unauthorized Receipt of Confidential Information

Each Center (or at the Bureau level, if more appropriate) should develop a procedure to address the receipt of confidential information, which it is not authorized to receive or which is more than the *minimum necessary* to achieve the intended purpose as described in section VI.A below. For example, this might include the receipt of an individual's name, when only a client identifier should be submitted.

The procedure for the unauthorized receipt of confidential information should, at a minimum, include provisions for:

1. Informing the disclosing party that the confidential information should not have been disclosed; and
2. Working with the disclosing party to determine if the confidential information should be destroyed or returned to the disclosing party.

III. Use and Disclosure of Confidential Information

As a hybrid entity under the Health Insurance Portability and Accountability Act (HIPAA), the Department must follow specific rules regarding the use and disclosure of confidential information between Department Bureaus and programs, and to third-parties outside MDPH.

[7] If the information is submitted by the data subject's personal representative, workforce members must verify that the individual submitting information is the personal representative in accordance with Procedure # 9: Verification of Individuals or Entities Requesting Disclosure of Confidential Information.

Use means access to or the release of confidential information:

- From a non-covered component to a covered component;
- From a non-covered component to a non-covered component;
- Within a non-covered component; or
- Within a covered component.

Disclosure means the release of confidential information:

- From a covered component to another covered component
- From a covered component to a non-covered component
- From a non-covered component to a third-party outside MDPH; or
- From a covered component to a third-party outside MDPH.

Use and Disclosure Matrix						
		Receiving Entity				
		Different CC	*Same CC*	*Different NCC*	*Same NCC*	*Third-Party*
Disclosing Program	***NCC***	Use	N/A	Use	Use	Disclosure
	CC	Disclosure	Use	Disclosure	N/A	Disclosure

The requirements for the *use* of confidential information are described in sections III.A and III.B. The requirements for the *disclosure* of confidential information are described in section III.C.

A. When Confidential Information May Not be Used

Confidential information *may not* be used:

1. For any of the purposes listed in section III.B if a consent form signed by the data subject, in order to participate in a MDPH program, limits the use of the information in a manner that conflicts with these purposes;
2. By MDPH workforce members for their own purposes, including, for example, a dissertation or other research including research in collaboration with outside researchers, without meeting the research requirements specified in Procedure # 6: Research Requirements; and
3. By any MDPH workforce members for their own purposes after leaving the workforce, unless in compliance with the MDPH Confidentiality Policy and Procedures.

B. When Confidential Information May be Used

The *use* of confidential information is limited to the following purposes:

1. Purposes authorized by law or regulation or that are consistent with the intent of the statute or regulation that required or authorized the reporting;
2. Purposes authorized in writing by the data subject based on a valid authorization as specified in Procedure # 4;
3. Research or scientific studies approved by the Commissioner pursuant to MGL c. 111, § 24A, or other statutes authorizing public health

research. The Department's requirements related to research are described in Procedure # 6; or

4. Program evaluation, quality improvement, payment verification, public health surveillance or other health care operations provided that the MDPH Intra-Department Data Use Agreement is executed between the program maintaining custody of the data and the program that intends to use the data. Whenever feasible, the data should be provided without identifiers or identifiers should be destroyed as soon as they are no longer required. A copy of the completed Intra-Department Data Use Agreement shall be held by each participating Center and filed by the primary custodian with the coordinator of RaDAR.
5. Workforce members shall not remove confidential information from the building including paper or electronic information, unless it is required for a field visit, meeting or otherwise necessary for work related purposes and only if pursuant to Center procedures. Appropriate measures shall be taken in each instance to insure that confidential information removed from the building is secured from unauthorized access.

C. When Confidential Information May be Disclosed

Disclosures of confidential information may only be made in the following circumstances:

1. The disclosure is required by law or regulation. Such disclosures must comply with and be limited to the requirements of the applicable law or regulation.
2. The disclosure is to a public health authority or health oversight agency that is authorized by law or regulation to collect or receive confidential information. Confidential information that may be disclosed to a public health authority when authorized by law or regulation includes, but is not limited to, information necessary for preventing or controlling disease, injury or disability, reporting vital records, federal grant compliance, or conducting public health surveillance, investigations or interventions. Confidential information that may be disclosed for activities related to oversight of the health care system, government health benefits programs, and entities subject to government regulations, when authorized by law or regulation, includes, but is not limited to, activities such as audits, civil and criminal investigations and proceedings, inspections, and licensure and certification actions.
3. The disclosure is to an appropriate governmental authority authorized by law to receive the reports of child abuse or neglect.
4. The disclosure is authorized in writing by the data subject in accordance with a valid authorization as specified in Procedure # 4.
5. The disclosure is to a vendor or agent of the Department pursuant to a contract to perform a governmental or public function or purpose. A covered component must execute a Business Associate Contract as

required by Procedure # CC-2: Business Associates Agreements. Non-covered components are not required to execute a Business Associate Contract. However, when there is sharing of confidential information with a contract vendor, language covering the use, disclosure and security of such information must be included when a contract is executed, as is described at http://healthnet/privsec/cagreements.htm.

6. The disclosure is required by judicial order or other legal process. Covered and non-components that receive subpoenas shall follow Procedure # 5: Responding to Subpoenas, which establishes uniform standards for responding to subpoenas. Procedure # 5 insures that confidential information related to data subjects is not released without the authorization of the data subject or a proper court order. All court orders for disclosure of confidential information shall be referred to the Office of the General Counsel, unless a different protocol is developed by the program in consultation with the Office of the General Counsel.
7. The disclosure is authorized by the Commissioner for research or scientific studies pursuant to MGL c. 111, § 24A, or other statutes authorizing public health research. A "Pledge of Confidentiality" must be signed and returned to the Department by all researchers who will have access to the data before confidential information is disclosed. Additional requirements related to research are described in Procedure # 6.
8. The confidential information has been de-identified in accordance with the requirements in Procedure # 7: De-Identification, Limited Data Sets, and Aggregate Data, and, if relevant, in accordance with Procedure # 8: Public Records Release Standards for Documents Containing Medical Information, unless the disclosure is otherwise restricted by law.
9. The confidential information has sufficient identifiers removed to qualify as a limited data set and the disclosure is subject to a Limited Data Set Agreement in accordance with the requirements in Procedure # 7. Disclosure of a limited data set is at the Department's discretion and must be reviewed by the Department's Research and Data Access Review (RaDAR) Committee.
10. The disclosure is for aggregate data that meets the aggregate data requirements in Procedure # 7.
11. When MDPH serves as a direct health care provider, certain confidential information may be disclosed to: (a) other health providers for treatment purposes pursuant to patient approval; and (b) under limited circumstances to family members or friends involved in the care of the individual, as permitted by law.
12. The disclosure pertains to identifiable vital record information that is considered unrestricted in accordance with applicable laws in M.G.L. c. 46 and is disclosed by the Registry of Vital Records and Statistics.

IV. Administrative Requirements Related to the Disclosure of Confidential Information

A. Processing Disclosures

All requests for disclosures of confidential information should be made in writing. Any disclosure pursuant to an authorization from a data subject must be in writing, signed by the data subject or personal representative.

Any Center that receives a request for the disclosure of confidential information for research purposes or as a limited data set must contact the Coordinator of RaDAR Committee. A copy of each request shall be provided to the Coordinator. All other requests shall be processed by individual centers.

B. To Whom Confidential Information May be Disclosed

Confidential information may only be disclosed for the purposes listed in section III.C and only to an individual authorized to receive the information. Prior to the release of confidential information, each workforce member responsible for the disclosure shall verify the identity of the data subject or the individual authorized to receive confidential information as required by Procedure # 9: Verification of Individuals or Entities Requesting Disclosure of Confidential Information.

C. Record of Disclosures

Each Center shall develop a procedure for recording all disclosures of confidential information. This record will provide the basis for the accounting of disclosures that each Center must produce in response to a data subject's request as described in Procedure # 12: Accounting of Disclosures. The record of disclosures can be produced by:

- Maintaining a paper or electronic disclosure log, which tracks each disclosure required in an accounting as they are made; or
- Utilizing existing Center records to compile the required accounting upon receipt of a data subject's request.

D. Questions Concerning Disclosures

Questions concerning whether a request for disclosure satisfies the disclosure criteria specified above should be addressed to the Office of the General Counsel or the Privacy Office.

V. Security Standards for Confidential Information

As required by Procedure # 10: Security of Confidential Information, all confidential information shall be collected, maintained, used and disclosed in a secure manner and,

whenever feasible, destroyed or de-identified when the confidential information no longer must be retained as required by the Records Conservation Board.[8]

VI. Minimum Necessary and Role-Based Access Standards

A. Minimum Necessary

Centers[9] shall take reasonable measures to ensure that the amount of confidential information collected, used and disclosed by authorized persons is limited to the *minimum necessary* to complete his or her job functions.

1. Determining Minimum Necessary

Generally, Centers will determine the minimum necessary confidential information by reviewing the requirements of the statute, regulation, authorization, grant or research proposal governing their collection, use or disclosure of information. In these instances, the minimum necessary confidential information will consist of the elements so specified or necessary to achieve the intended purpose.

Centers may also rely, in their discretion, on the judgment of a party making the request regarding the amount of confidential information to be released if it is:

- A covered entity under HIPAA;
- A public official, as permitted under 45 C.F.R § 164.512, for public health reporting;
- A health care provider for treatment purposes;
- An individual or organization for research purposes, if the request is approved by RaDAR; or
- HHS pursuant to a privacy investigation.

2. Center Minimum Necessary Procedures

Centers shall develop procedures for the following categories of disclosures:

a. For each *routine and recurring* disclosure of confidential information each Center shall create a list or matrix that describes:

- The minimum necessary elements to be disclosed;
- The purpose of the disclosure; and
- The recipient of the disclosure.

[8] Information related to the Massachusetts Records Conservation Board is available at http://www.state.ma.us/sec/arc/arcrcb/rcbidx.htm.

[9] Throughout the Confidentiality Policy and Procedures most references are to Centers. Where appropriate, procedures may be developed at the Bureau or program level, with the approval of the Center Director.

b. For *non-routine disclosures* of confidential information, each Center shall develop procedures for reviewing and approving non-routine disclosures to ensure they meet the minimum necessary standards.

B. Role-Based Access

Workforce members in each Center should have access to only those physical and electronic records containing confidential information that are required for their job functions and for which they are granted access rights.

1. Role-Based Access Procedures

Each Center shall establish specific procedures for ensuring compliance with the role-based access standard. The procedures shall describe the processes for:

- Insuring that authorized users review, forward and/or print only those fields and/or records relevant to the workforce member's job functions;
- Granting and approving access rights to information systems; [10]
- Reviewing and auditing role-based access rights;
- Modifying access rights when necessary; and
- Terminating access rights following a workforce member's resignation or termination.

2. Role-Based Access Personnel Lists

Each Center shall maintain a list of all workforce members, or categories of workforce members,[11] with access rights to confidential information. The list must be updated as necessary, and should be shared with IT services for the respective center, to ensure authorized access to electronic confidential information. Each role-based access list must include the following elements:

- Employee name;
- Job title or functions;
- Name and location of data accessed;
- Employee's access level and rights;
- Time or frequency of access; and
- Access and authentication controls.

Authority: M.G.L. c. 66A, § 2
45 C.F.R. §§ 164.502 and 164.506-512

Forms: Intra-Department Data Use Agreement

[10] Temporary employees, interns, and volunteers shall not be granted access to confidential information, unless first authorized by the supervisor in charge of such individuals and then approved by the Program or Hospital Director.

[11] The list may be maintained by category, provided that all workforce members have identical access rights and the Center can identify all workforce members in each category.

Procedure Title:	Authorizations for the Use and Disclosure of Confidential Information		
Procedure Number:	4	**Version #**	2.0
Effective Date:	May 3, 2004		

Content

I. Purpose and Scope

This procedure describes the required form, and the elements that must be included in any authorization received by and acted on by MDPH and its vendors, unless subject to other legal restrictions or requirements. This procedure applies to all covered and non-covered components, and all Department workforce members. Individual provisions of the procedure apply to only covered or non-covered components as described below.

II. MDPH Authorization Forms: General Requirements

Uses and disclosures other than those described in Procedure # 3: Use and Disclosure of Confidential Information require a signed authorization. An authorization is a form signed by a data subject or their personal representative that allows another person or entity to collect, use or disclose the data subject's confidential information, unless subject to other legal restrictions or requirements.

A. When requesting confidential information, all Centers shall use authorization forms that contain the core elements described in section III below. MDPH Centers may utilize the Department's model authorization form, or develop program-specific authorizations containing, at a minimum, the core elements in

consultation with the Office of the General Counsel. Any program-specific authorization must be available to the Privacy Office upon request.

B. Any MDPH program that is seeking authorization to obtain confidential health information from any outside entity that is a HIPAA covered entity must use an authorization that contains all the above listed core elements.

C. Any MDPH program that provides authorization forms to its vendors must provide an authorization form that contains all the above listed core elements.

D. Any disclosure to a legislator regarding a constituent's confidential information requires an authorization.

III. Core Elements of a Valid Authorization

A. Before releasing information pursuant to an authorization, the workforce member must be sure that the authorization contains at a minimum the following ten (10) required elements:

1. A description of the information to be used or disclosed that identifies the information in a specific and meaningful way;
2. The name or other specific identification of the category of person or person(s) authorized to make the requested use or disclosure;
3. The name or other specific identification of the category of person or person(s) to whom the requested use or disclosure may be made;
4. A description of the purpose of the disclosure or a statement that the disclosure is at the request of the data subject, when the data subject initiates the authorization and does not choose to state a purpose;
5. An expiration date or expiration event that relates to the data subject or the purpose of the use or disclosure (i.e., "the end of research study");
6. A statement regarding the data subject's right to revoke the authorization in writing, including a description of the process for revoking the authorization. It must also include a statement that information previously released in reliance upon the authorization is not affected by the revocation;
7. A statement regarding the conditioning of the authorization. Generally, the provision of treatment, payment or enrollment or eligibility for benefits cannot be conditioned on signing the authorization. However, research-related treatment; health plan enrollment or the determination of eligibility for benefits; or the provision of health care that is solely for the purpose of creating confidential health information for disclosure to a third party may be conditioned on signing an authorization;
8. A statement that there is potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient, who may not be subject to state or federal privacy laws;
9. The signature of the individual and the date; and
10. If the authorization is signed by a personal representative of the data subject, a description of the representative's authority to act on the individual's behalf.

IV. Review of Authorizations from Entities Requesting Confidential Information

A. General Requirements

1. Before disclosing the information pursuant to the authorization, workforce members must first determine if the authorization is valid as described in this section.
2. Next, workforce members should verify the identity of the requesting party as described in Procedure # 9: Verification of Individuals or Entities Requesting Disclosure of Confidential Information.
3. After determining that the authorization is valid and the identity of the requesting party, the workforce member should release only the information specifically listed on the authorization form.
4. If there are questions on how to proceed or about whether the authorization is valid contact the Office of the General Counsel or the Privacy Office.

B. Covered Components

Upon receipt of an authorization, the MDPH workforce member(s) in covered components responsible for the requested records shall review the authorization to determine if it is valid by verifying that the authorization:

1. Contains all the core elements listed in section III;
2. Has not expired;
3. Is fully completed;
4. Is not improperly conditioned as described in section III.A.7, and section VII.B;
5. Is not incorrectly combined with another document as described in section VII;
6. Is properly signed by the data subject or personal representative;
7. Does not contain any information that is known to be false; and
8. Has not been revoked.

C. Non-Covered Components

All non-covered component programs are strongly encouraged to require that authorizations submitted to the program contain all the core elements listed in section III. However, non-covered component programs retain the discretion to act on an authorization that does not meet this standard, upon review and approval by the program director as described below.

If a non-covered component program receives an authorization that does not contain all of the required core elements, it may return the authorization and require a compliant one. However, a non-covered component may, in its discretion, review the authorization with the program director or her designee, and decide to honor it if it is deemed sufficiently complete. The reasons for honoring the authorization shall be documented in writing and maintained by the program along with the authorization. The program shall adopt appropriate guidelines if it allows the release

of confidential information pursuant to such authorizations on other than a non-routine basis. A copy of such guidelines must be available to the Privacy Office upon request.

D. Authorizations for Information Held by More Than One Program

If the authorization covers information held by more than one program, it shall be coordinated among the programs, with the program maintaining the most records taking the lead. If multiple programs are involved, which include both covered and non-covered components, contact the Privacy Office.

V. Copies of Authorization Forms

A. An original authorization form is preferred for disclosure of confidential information; however, a clear and legible photocopy or facsimile is acceptable.

B. If MDPH is seeking an authorization from a data subject, it must provide a copy of the authorization form to the data subject.

C. If MDPH is releasing or using information pursuant to an authorization form, it must maintain a copy of the form. All forms must be maintained for a minimum of six years, or as required by the Records Conservation Board.[12]

VI. Additional Protections for Certain Confidential Information

A. HIV/AIDS Records

Information regarding the release of HIV/AIDS diagnosis or HIV/AIDS treatment is protected by M.G.L. c. 111, § 70F. No health care facility may release such records without separate informed consent, which shall be distinguished from the written authorization for the release of any other medical information. Therefore, such information shall not be released without specific authorization, separately acknowledged, or the use of a separate authorization form.

B. Genetic Information

Information regarding the release of genetic information is protected by M.G.L. c. 111, § 70G. No health care facility may release such records without separate informed consent, which shall be distinguished from the written authorization for the release of any other medical information. Therefore, such information shall not be released without specific authorization, separately acknowledged, or the use of a separate authorization form.

[12] Information related to the Massachusetts Records Conservation Board is available at http://www.state.ma.us/sec/arc/arcrcb/rcbidx.htm.

C. Substance Abuse Records

Records that contain information concerning alcohol or drug treatment are protected by 42 C.F.R. Part 2. The federal standards for the release of records containing information about alcohol or drug treatment are very specific and in some instances stricter than HIPAA. Therefore, such information shall not be released without specific authorization, separately acknowledged, or the use of a separate authorization form. Any authorization for information concerning alcohol or drug treatment must also include a separate notice prohibiting the redisclosure of the confidential information.

VII. Combining an Authorization Form with Another Authorization or Document

A. Psychotherapy Notes[13]

A separate authorization form for the use and disclosure of psychotherapy notes is required. It cannot be combined with a general authorization for release of confidential information.

B. Pre-Condition

An authorization that a covered entity has required as a condition for treatment, payment, eligibility for benefits, or enrollment in a health plan cannot be combined with another authorization.

C. Research

An authorization for use and disclosure of confidential information for research may be combined with any informed consent form for the same research study.

Authority: 45 C.F.R. §§ 164.508 and 164.532(a)-(c)
Forms: Model Authorization Form

[13] Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the content of conversations during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Procedure Title:	Responding to Subpoenas		
Procedure Number:	5	**Version #**	2.0
Effective Date:	May 3, 2004		

Content

I. Purpose and Scope

This procedure establishes uniform standards for responding to subpoenas[14], ensuring that confidential information related to data subjects is not released without the authorization of the data subject or a proper court order.[15] This procedure applies to both covered and non-covered components of the Department and all Department workforce members.

As described in section IV, the Fair Information Practices Act (FIPA) establishes a stricter standard for the release of information pursuant to a subpoena than does the Health Insurance Portability and Accountability Act (HIPAA). The FIPA standard will be followed by all parts of the Department responding to subpoenas, regardless of whether the Center or program is a covered health care component under HIPAA.

II. Procedure for Responding to Subpoenas

Workforce members should refer to the flow chart at end of procedure when reviewing the procedure for responding to subpoenas described in this section.

[14] Subpoena means a formal request to compel the Department to produce an individual to testify or to produce documents in relation to a proceeding in which the Department may or may not be a party to the action. A subpoena may be issued by an attorney or, in some instances, by the court. It is often accompanied by a witness fee. Failure to respond to a subpoena may result in legal sanctions.

[15] M.G.L. c. 66A, § 2(k) provides that holders of personal data are required to "maintain procedures to ensure that no personal data are made available in response to a demand for data made by means of compulsory process, unless the data subject has been notified of such demand in reasonable time that he may seek to have the process quashed."

A. Determine if the Request is a Court Order

Determine whether there is a court order for the release of the information, alone or in combination with a subpoena. Court orders are outside the scope of this procedure. Programs that routinely receive court orders may work out a protocol with the attorney for the program regarding how to process them. In the absence of a protocol, court orders should be referred to the Office of the General Counsel (OGC) and will be considered on a case by case basis.

B. Contact the Office of General Counsel

Upon receipt of a subpoena (without a court order) notify the Office of General Counsel (specifically the attorney for the program receiving the subpoena) unless a standard protocol as described in section III is developed in consultation with the program's attorney, which does not require notice in each instance.

C. Determine If the Subpoena Seeks Personal Data or a Public Record

Determine whether the subpoena seeks personal data that is subject to FIPA or whether the information constitutes a public record. Information that constitutes a public record may be released.

D. Determine if the Subpoena Seeks Personal Data and Includes an Authorization

If the subpoena seeks personal data, determine if it is accompanied by an authorization for the release of personal data that complies with Procedure # 4: Authorizations for the Use and Disclosure of Confidential Information. If there is a compliant authorization, information specified in the authorization may be released using sample letter # 3.[16]

E. Determine the Type of Personal Data Sought

If the subpoena is for documents that contain personal data and there is no authorization from the data subject allowing the disclosure, determine whether the personal data is medical information or other personal data (non-medical information).

1. If the subpoena is for information that is non-medical information and it can be de-identified in compliance with Confidentiality Procedure # 7: De-Identification, Limited Data Sets and Aggregate Data and still be responsive to the request, the documents may be released after they are fully de-identified using sample letter # 3.

2. If the subpoena is for documents that contain personal data that are;
   - Medical information; or
   - Non- medical information that cannot be de-identified; and

[16] The sample letters referenced in this procedures are at http://healthnet/privsec/forms.htm.

- There is no authorization from the data subject allowing the disclosure of information;

The documents *cannot* be released unless the data subject authorizes the release or a court[17] orders the release.

F. Contact the Data Subject

Contact the data subject(s) regarding the subpoena. Use sample letter # 1 to give notice that the Department received a subpoena requesting personal data about the data subject. Also, include:

1. An authorization to release the information (using the MDPH Model Authorization form); and
2. The date by which the data subject should respond with the authorization, move to quash the subpoena or seek a limiting or protective order from the court.

G. Notify the Issuing Attorney

At the same time that the data subject is notified, notify the attorney issuing the subpoena using sample letter # 2, that:

1. Pursuant to M.G.L. c. 66A, § 2(k), notice was given to the data subject(s);
2. The Department cannot release requested documents unless the data subject authorizes the release or there is a proper court order requiring the release of the documents[18]; and
3. The Department will contact the attorney if authorization is received, or by a date specific if no response is received.

H. The Data Subject's Response to the Subpoena

The Department's final actions will depend on the data subject's response to the subpoena.

1. If the data subject provides authorization for the release of the personal data, use sample letter # 3 to release the requested documents to the attorney issuing the subpoena.
2. If the data subject moves to quash the subpoena or for a limiting or protective order, wait for the decision of the court. If the court orders the release of the documents contact the OGC. Release the requested documents pursuant to the directions of the court order.
3. If the data subject fails to respond to the letter requesting authorization within the time frame provided, use sample letter # 4, to notify the attorney that the data subject did not respond, and that the Department cannot release the documents without a court order, in the absence of the data subject's authorization. This letter should also be sent (as a cc) to the court where the case is filed, if this information can be identified from the subpoena. If the

[17] Court refers to a federal or state court, and does not include an administrative tribunal. A court order is an order issued by a judge of the court.
[18] Allen v. Holyoke Hospital, 398 Mass. 372, 496 N.E.2d 1368 (1986).

subpoena contains specific information about the case, including the caption and index number, these should be included as a means to identify the case.

4. If the Department receives a court order, contact the OGC. Release the requested documents pursuant to the directions of the court order.

III. Establishing Protocols

Programs that handle many subpoenas should work with the program's attorney to establish a protocol of how to process routine subpoenas including, when the program should contact the attorney.

IV. HIPAA: Subpoena Requirements

A. General Requirements

Under HIPAA, a covered entity may release information pursuant to a subpoena that is *not* authorized or accompanied by a court order, if it receives a "satisfactory assurance"[19] as described in section IV.B. FIPA has a more restrictive standard, requiring the data subject's authorization or a court order before the Department may release information pursuant to a subpoena. The FIPA standard will be followed by all parts of the Department responding to subpoenas, regardless of whether the Center or program is a covered health care component under HIPAA. However, as described in section IV.C, the Department must follow the requirements of HIPAA when issuing a subpoena to a HIPAA covered entity.

1. Satisfactory Assurance from the individual
   - **a.** The party issuing the subpoena made a good faith attempt to provide written notice to the subject of the PHI, sufficient to permit the individual to raise an objection (mailing to individual's last know address is deemed sufficient); and
   - **b.** The time to raise objections has elapsed, and
     - No objections were filed; or
     - All objections filed were resolved by the court or administrative tribunal, and disclosures are consistent with the resolution.

2. Satisfactory Assurance that steps were taken to secure a qualified protective order[20]
   - **a.** The parties have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

[19] 45 C.F.R. § 164.512(e)(1)

[20] An order of a court or an administrative tribunal or a stipulation by the parties to the litigation that (a) prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which it was requested; and (b) requires the return to the covered entity or destruction of the PHI at the end of the litigation or proceeding.

b. Party seeking PHI requested a qualified protective order from such court or tribunal.

B. Subpoenas Issued by the Department

Subpoenas issued by the Department to a HIPAA covered entity must be accompanied by a certification of satisfactory assurance. An attorney in the OGC will prepare the required documentation, depending on the circumstances. Proof of steps taken in the satisfactory assurance process, as described above, shall be kept in the file, including for example:

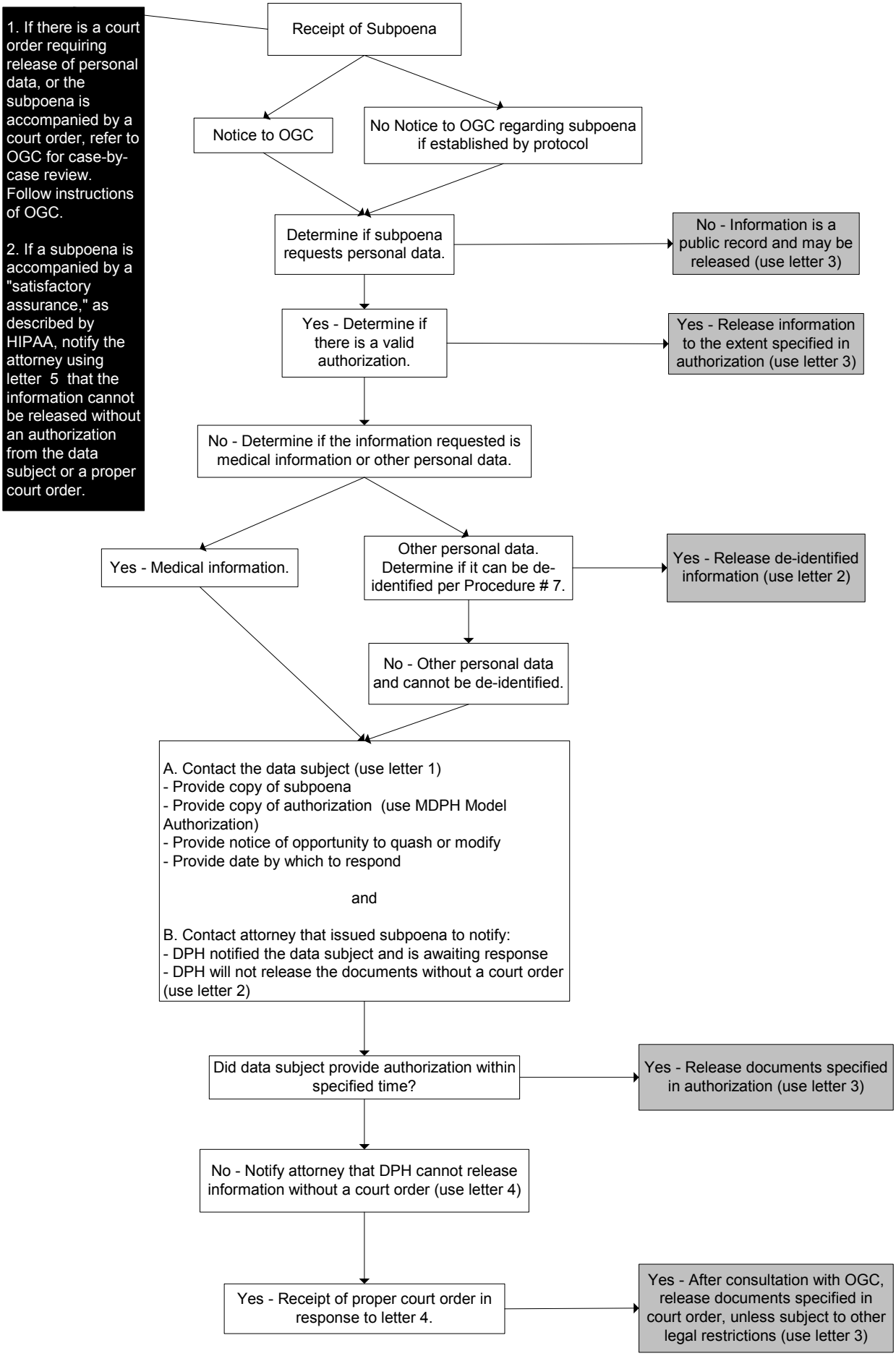
- Written notice to data subject;
- Proof of mailing, including the date of mailing (certificate of mailing or certified mailing receipt) to the data subject; and
- Qualified protective order submitted to court.

C. Subpoenas Received by the Department

If a subpoena is accompanied by a "satisfactory assurance," which meets only the HIPAA, and not the FIPA standard, notify the attorney using sample letter # 5 that the Department is subject to FIPA and cannot release the information without an authorization from the data subject or a proper court order.

Authority: M.G.L. c. 66A, § 2(k)
45 C.F.R. § 164.512(e)

Forms: Sample Letter # 1
MDPH Model Authorization
Sample Letter # 2
Sample Letter # 3
Sample Letter # 4
Sample Letter # 5


1. If there is a court order requiring release of personal data, or the subpoena is accompanied by a court order, refer to OGC for case-by-case review. Follow instructions of OGC.
2. If a subpoena is accompanied by a "satisfactory assurance," as described by HIPAA, notify the attorney using letter 5 that the information cannot be released without an authorization from the data subject or a proper court order.
Receipt of Subpoena
Notice to OGC
No Notice to OGC regarding subpoena if established by protocol
Determine if subpoena requests personal data.
No - Information is a public record and may be released (use letter 3)
Yes - Determine if there is a valid authorization.
Yes - Release information to the extent specified in authorization (use letter 3)
No - Determine if the information requested is medical information or other personal data.
Yes - Medical information.
Other personal data. Determine if it can be de-identified per Procedure # 7.
Yes - Release de-identified information (use letter 2)
No - Other personal data and cannot be de-identified.
A. Contact the data subject (use letter 1)
- Provide copy of subpoena
- Provide copy of authorization (use MDPH Model Authorization)
- Provide notice of opportunity to quash or modify
- Provide date by which to respond
and
B. Contact attorney that issued subpoena to notify:
- DPH notified the data subject and is awaiting response
- DPH will not release the documents without a court order (use letter 2)
Did data subject provide authorization within specified time?
Yes - Release documents specified in authorization (use letter 3)
No - Notify attorney that DPH cannot release information without a court order (use letter 4)
Yes - Receipt of proper court order in response to letter 4.
Yes - After consultation with OGC, release documents specified in court order, unless subject to other legal restrictions (use letter 3)

Procedure Title:	Research Requirements		
Procedure Number:	6	**Version #**	2.0
Effective Date:	May 3, 2004		

Content

I. Purpose and Scope

This procedure describes the Department's requirements relating to research, as defined in the glossary to the Department's Confidentiality Policy and Procedures, that is conducted by Department workforce members or authorized by the Department, including:

- Granting authorization for public health research pursuant to M.G.L. c. 111, § 24A;
- Allowing access for research purposes to confidential information maintained by MDPH, including birth records (M.G.L. c. 111, § 24B), fetal death records (M.G.L. c. 111, § 202), cancer registry data (M.G.L. c. 111, § 111B), birth defects surveillance data (M.G.L. c. 111, § 67E), and other databases containing confidential information; and

- Ensuring adequate protection of human research subjects and confidential information as well as determining when review of a research protocol by the MDPH Human Research Review Committee is necessary.

As described in section II, this procedure applies only to research projects that are either conducted or authorized by the Department. It does not apply to surveillance, disease or injury investigation or other public health practices routinely performed by the Department's workforce[21] in fulfilling statutory mandates or the Department's mission. While this procedure does not apply to the public health practices conducted by MDPH workforce, other confidentiality procedures mandating the appropriate safeguards for these projects do apply.

The provisions of this procedure apply to both covered and non-covered components of the Department and all workforce members conducting research, unless otherwise indicated.

II. Non-Applicability to Public Health Practice

Determinations about whether a particular project constitutes research or public health practice, or some combination of the two, must be made on a case-by-case basis. Questions related to the distinction between research and public health practice should be directed to the Office of the General Counsel.

As general guidance, the U.S. Centers for Disease Control and Prevention (CDC) notes that the major difference between research and public health practice lies in the primary intent of the activity.[22] Under federal regulations the primary intent of *research* is the "systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge."[23] However, the primary intent of *public health practice* is the prevention of disease or injury to the public and the improvement of public health.

Certain traditional public health activities, including surveillance, emergency response, and program evaluation, may be research or public health practice depending on the intent of the investigation. In general, a project is *research* if it is primarily intended to generate generalizable knowledge concerning public health; the intended benefits of the project may or may not include study participants but always extend beyond the study participants to the larger population; and data collected exceed the requirements for care of the study participants. In contrast, a project is generally considered *public health practice* if the primary intent of the project is to identify and control a health problem; the intended benefits of the project are primarily or exclusively for the study

[21] Workforce for the purposes of Procedure # 6 refers to MDPH staff and agents.
[22] U.S. Centers for Disease Control and Prevention, *Guidelines for Defining Public Health Research and Public Health Non-Research*, at http://www.cdc.gov/od/ads/opspoll1.htm (last revised Oct. 4, 1999).
[23] 45 C.F.R. § 46.102

participants; data collected are needed to assess and/or improve the health of the participants; and the project activities are not experimental.

III. Section 24A Authorization for Public Health Research

Approval from the Commissioner of Public Health pursuant to M.G.L. c. 111, § 24A is required for research conducted by MDPH workforce or research involving access to or the use of MDPH and non-MDPH confidential information.

M.G.L. c. 111, § 24A authorizes the Commissioner of MDPH to approve "scientific studies and research which have for their purpose the reduction of morbidity and mortality within the Commonwealth." Generally, receiving § 24A approval provides the following protections:[24]

- Any data or information collected for purposes of the research are treated as confidential. It protects such information from release under the public records law;
- The persons and institutions providing the data or information are immune from liability resulting from their release; and
- The data or information are not admissible as evidence in any litigation or other legal proceeding.

For studies that are not conducted by MDPH workforce and do not involve access to confidential data maintained by MDPH, the Department generally does not grant § 24A approval. Researchers not affiliated with MDPH, who wish to protect the confidentiality of sensitive data collected from sources outside of MDPH, may be eligible to apply for a Federal Certificate of Confidentiality pursuant to 42 U.S.C. § 241(d).[25]

A. Requests for § 24A Approval by MDPH Workforce

1. Application Requirement

MDPH workforce members who intend to conduct research or a study must submit a complete *Application by MDPH Workforce for Commissioner Authorization for Public Health Research or Study* to the Coordinator of the Research and Data Access Review Committee (RaDAR). The application requires detailed information about the study protocol, justification for variables requested, measures to ensure the confidentiality and security of the data, and documentation of the Department's Institutional Review Board (Human Research Review Committee), if required. If a project requires access to data from another

[24] It is important to note that § 24A approval may not protect the data or information from subpoena by a criminal defendant, and may not protect persons and institutions providing the data or information when those persons or institutions are located outside of Massachusetts.

[25] Additional information on Federal Certificates of Confidentiality is at: http://grants2.nih.gov/grants/policy/ coc/index.htm.

state agency, the workforce member must comply with all requirements of the other agency as well as coordinate the data request with RaDAR.

Note: All MDPH workforce members that want to use MDPH confidential information for their own purposes, including, for example, a dissertation or other work including research in collaboration with outside researchers, are required to follow the procedures described in section III.B for researchers not affiliated with MDPH.

2. Standard Review Process

The application is initially reviewed by RaDAR or a sub-committee of RaDAR. The RaDAR Committee or sub-committee will request clarification or additional information from the researcher when necessary to complete the review of the study. Once this review is complete, the application must be recommended for approval by the RaDAR Committee or sub-committee, the Office of the General Counsel, and the Office of Policy and Planning, before it is submitted to the Commissioner for approval.

3. Expedited § 24A Review

In very limited circumstances when a MDPH project relates to an urgent matter, a § 24A application by MDPH workforce may receive an expedited review by the Office of the General Counsel and the Office of Policy and Planning with input as necessary from other appropriate individuals. In such situations, the Office of the General Counsel and the Office of Policy and Planning are authorized to determine whether or not to recommend approval by the Commissioner without review by the RaDAR Committee.

4. Approval

RaDAR's recommendation is forwarded to the Commissioner for § 24A approval. Approved researchers are required to agree to certain conditions and limitations on the use and disclosure of confidential information obtained as part of the research study.

B. Requests for § 24A Approval from Researchers Not Affiliated with MDPH

The Department has a separate application, review and approval process for researchers who are not affiliated with MDPH that seek § 24A approval for access to confidential MDPH data. To request § 24A approval, a researcher not affiliated with MDPH must submit a complete "Application for Authorization for Public Health Research," available from the MDPH RaDAR Coordinator. The application requires detailed information about the study protocol, justification for all variables requested, measures to ensure the confidentiality and security of the data, and documentation of appropriate Institutional Review Board approval. The application is reviewed by the full RaDAR Committee, which after seeking any necessary clarifications from the researcher will recommend to the Commissioner whether or not to approve the study. Approved researchers are required to enter into an

agreement with MDPH establishing the conditions and limitations on the use and disclosure of confidential information obtained as part of the research study. All co-investigators in the study who have access to confidential information are required to sign a confidentiality agreement.

C. Criteria for § 24A Approval

Approval of a § 24A application is at the discretion of the Commissioner, and is determined on a case-by-case basis. In general, a study is not appropriate for § 24A approval if:

- It is not likely to lead to results which could contribute to the reduction of morbidity or mortality in the Commonwealth;
- It is primarily an internal program evaluation;
- It is primarily a routine surveillance activity conducted pursuant to a statutory or other legal mandate;
- All the data required to conduct the research are publicly available or not confidential; or
- It does not have a clearly defined purpose, the application is vague or incomplete, or the application fails to demonstrate adequate measures for securing confidential data.

Appendix A provides a complete list of review criteria.

IV. Access to Confidential MDPH Data for Research Purposes

All requests for access to MDPH confidential data also include a review and require an approval pursuant to § 24A, as described in section III. However, the RaDAR chair, in consultation with the RaDAR coordinator and the Office of the General Counsel, has the discretion in limited circumstances to approve the release of certain data as a Limited Data Set for research purposes rather than requiring a § 24A review, provided that the data qualify as a Limited Data Set, there is minimal risk of identification of data subjects, there is no data subject contact, and a Limited Data Set Agreement is executed.

The Department maintains numerous public health databases and registries containing confidential information that is exempt from disclosure as a public record,[26] but is available to researchers under certain conditions. Anyone requesting access to MDPH confidential databases for research must complete the appropriate application and submit it to the MDPH RaDAR coordinator. The process for requesting access to several MDPH databases is described below. For access to other MDPH databases, researchers should contact the RaDAR coordinator, who will work with the program holding the requested information.

[26] M.G.L. c. 4 § 7, clause 26; and M.G.L. c. 66.

A. Birth Records and Fetal Death Records

M.G.L. c. 111, § 24B requires reporting of birth information to the Department. M.G.L. c. 111, § 202 requires reporting of most fetal deaths to the Department. These confidential records are available for statistical and research purposes only. Anyone requesting access to these confidential records for research purposes must submit a written application (available from the MDPH RaDAR Coordinator) for access to confidential data that combines § 24A approval with a request for confidential birth records (§ 24B) or fetal death records (§ 202). The application must undergo a formal review process as described above for § 24A.

B. Massachusetts Cancer Registry Records

M.G.L. c. 111, § 111B established the Massachusetts Cancer Registry, which requires reporting to the MDPH information related to malignant diseases and benign brain-related tumors that occur in Massachusetts residents. The information maintained by the cancer registry is confidential, but may be released for research purposes. Anyone requesting access to these confidential records for research purposes must submit a written application for access to confidential Massachusetts cancer registry data which combines § 24A approval with a request for confidential cancer registry information (§ 111B). The application must undergo a formal review process as described above for § 24A.

C. Massachusetts Birth Defects Monitoring Program Records

M.G.L. c. 111, § 67E requires reporting to the MDPH information related to birth defects that occur to Massachusetts residents. The information maintained by the Massachusetts Birth Defects Monitoring Program is confidential, but may be released for research purposes. Anyone requesting access to these confidential records for research purposes must submit a written application for access to confidential Massachusetts birth and birth defects data which combines § 24A approval with a request for confidential birth record information (§ 24B) and confidential birth defects information (§ 67E). The application must undergo a formal review process as described above for § 24A.

V. Federal Requirements for the Protection of Human Research Subjects

In addition to Massachusetts and federal laws that govern the disclosure of confidential information, the federal government has issued regulations protecting the rights and privacy of human subjects involved directly or indirectly in research.[27] These regulations (known as the Common Rule) apply only to "research involving human subjects," which is research involving any form of contact with an individual, an individual's next of kin or access to that individual's private records, including medical records.[28] The Common Rule also specifies when such review must be conducted by a full Institutional

[27] 45 C.F.R. Part 46 at http://ohrp.osophs.dhhs.gov/humansubjects/guidance/45cfr46.htm.

[28] Under the Common Rule, research is defined as the "systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge."

Review Board (IRB) committee and when it can be reviewed on an "expedited" basis because the research project involves no more than minimal risk to the research subjects.[29]

A. MDPH Workforce Researchers

In addition to other applicable research requirements, research conducted by MDPH workforce that is considered higher risk to human subjects, as described in section V.C and in Appendix B must be reviewed by the Department's IRB, known as the Human Research Review Committee (HRRC).[30]

B. Researchers Not Affiliated with MDPH

For research projects that involve collaboration with researchers at other institutions, the IRBs at the other institutions involved in the research project may also require their own review. Researchers not affiliated with MDPH are responsible for obtaining review by their sponsoring institution's IRB, which in most cases, the Department will require before granting § 24A approval. For certain research projects that are considered higher risk to human subjects, as described in section V.C and in Appendix B, and are conducted by researchers who are not affiliated with MDPH, the Department may require review and approval by the MDPH HRRC in addition to approval by the sponsoring institution's IRB.

C. Criteria for Review by Human Research Review Committee

HRRC's review criteria for human subject research are listed in Appendix B. In general, studies involving higher risk to human subjects and studies conducted by or in some manner sponsored by the MDPH will require a greater level of review. Appendix B should be used by researchers as guidance for when Commissioner approval pursuant to § 24A and MDPH HRRC review are necessary. The level of review required by MDPH is based upon:

1. The potential risk to human subjects who are either involved in the research and/or whose confidential data are being utilized; and
2. The affiliation of the researchers to the MDPH.

"Research involving human subjects" is defined as any research involving a "living individual about whom an investigator conducting research obtains:

1. Data through intervention or interaction with the individual; or
2. Identifiable private information."

See 45 C.F.R. §§ 46.102(d) & (f).

[29] One of these activities qualifying for expedited review is the study of existing data, documents, records, pathological specimens, or diagnostic specimens (i.e., no direct patient contact is involved).

[30] The Common Rule's requirements apply not only to any federal government research or any research funded by the federal government, but also to institutions which have signed an "assurance" with the federal Department of Health and Human Services. MDPH has signed such an assurance (Federal-Wide Project Assurance (FWA) # FWA00000786), and is obligated to comply with these federal regulations when dictated by the terms of the assurance document.

VI. Authorizations for Disclosures for Research

A. Covered Components

Under the federal Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, all researchers requesting confidential data held by a covered component of the Department must obtain either:

1. A signed authorization from each study subject as described below; or
2. A waiver of authorization[31] as described below.

B. Non-covered components

Researchers requesting access to confidential data from non-covered components of the Department are exempt from the requirement to obtain an authorization or waiver of authorization approved by an IRB. However, for studies involving contact with data subjects using Department data, the RaDAR Committee must determine as part of the project review that the study meets the waiver criteria as described in VI.C.2.e (excluding the IRB statement), prior to approving access to the confidential data.

C. Authorization Requirements

1. Written Authorization

Researchers must obtain from study subjects whose confidential information will be used in the research:

a. A valid authorization as specified in Procedure # 4: Authorization for Use and Disclosure of Confidential Information; or

b. A signed research informed consent form that contains the required elements of an authorization as specified in Procedure # 4.

or

2. Waiver of Authorization

As an alternative to a written authorization from each study subject, researchers may obtain a written waiver of authorization approved by an IRB. The written waiver must include:

a. The date of the waiver;

b. The signature of the IRB Chair or other authorized designee of the Chair;

c. A statement indicating whether the waiver was approved by expedited or full committee review;

d. A brief description of the confidential information for which use or disclosure has been determined to be necessary by the IRB ; and

e. A statement that the IRB determined that there is no more than a minimal risk to the privacy of individuals based on, at least, the presence of the following elements:

[31] 45 C.F.R. § 164.512(i)(2).

- An adequate plan to protect the identifiers from improper use and disclosure;
- An adequate plan to destroy identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining identifiers, or such retention is otherwise required by law;
- Adequate written assurances that the confidential information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of confidential information would be permitted;
- A determination that the research could not practicably be conducted without the waiver of authorization; and
- A determination that the research could not practicably be conducted without access to and use of the confidential information.

VII. Accounting of Disclosures for Research

As described in Procedure # 12: Procedures for Accounting of Disclosures, each Center that discloses confidential information for research must establish procedures to account for such disclosures unless, in accordance with Procedure #7: De-identification, Limited Data Sets and Aggregate Data, the information is rendered de-identified prior to disclosure, or sufficient identifiers are removed so that the information constitutes a limited data set.

Authority: M.G.L. c. 111, §§ 24A; 24B; 202; 111B; 67E
45 C.F.R. Part 46
45 C.F.R. § 164.512(i)

The Research and Data Access Review (RaDAR) Committee may recommend approval of an application for § 24A, § 24A/B, § 24A/B/202, § 24A/111B, or § 24A/B/67E only if it first determines that:

1. The application demonstrates:
- That the proposed study addresses a topic of public health and/or medical importance; and
- That the results of the proposed study may lead to the reduction of morbidity and mortality in the Commonwealth; and

2. The application demonstrates that the proposed study has sufficient scientific and methodological rigor to yield results which can be used to reduce morbidity and mortality in the Commonwealth; and

3. The study cannot be completed unless the researcher is able to obtain or have access to the information he or she is requesting; and

4. The researcher will not receive or obtain access to any more information than is absolutely necessary to complete the proposed research study and, if the study involves the transfer of confidential data from MDPH to the researcher, codes are aggregated where possible prior to transfer to minimize the amount of personal information transferred to the researcher; and

5. If the study involves the transfer of confidential data from MDPH to the researcher, the preparation of the data for the study is administratively feasible within MDPH; and

6. Informed consent of the data subject to release of personal or medical information is obtained whenever feasible; and

7. The application demonstrates that, without informed consent, no individual record data which could affect employment, or eligibility for health or insurance benefits will be provided to employers or insurers; and

8. If the study calls for patient contact:
- That appropriate patient contact protocols are in place; and
- That the patient contact protocols have been reviewed and approved by an Institutional Review Board (IRB) which meets the requirements of 45 C.F.R. Part 46; and

9. If the study involves the collection, testing and/or storage of human blood, urine, or tissue samples, the application includes a study protocol, approved by the sponsoring institution's IRB, that provides a response to each of the questions set forth in MDPH's *Research Involving Human Blood, Urine, or Tissue Collection for Analytical Testing and/or Storage*; and

10. The study protocol, together with the conditions the MDPH imposes on the study, provide adequate and appropriate safeguards to ensure the confidentiality of medical and other protected information; and

11. All persons who will have access to medical and other protected information shall sign written confidentiality agreements prior to their receipt of any such information; and

12. The application asserts that, at the completion of the research project, all confidential data provided by MDPH will be destroyed and no copies made or retained.

The process for determining the appropriate review requirements is as follows:

1. The risk levels described in the RaDAR (Research and Data Access Review Committee) and IRB (Institutional Review Board) Review Determination table listed below should be used as a guide for classifying the proposed research project into one of the four categories listed (Level I, IIA, IIB, or III). While some studies may not clearly match the types of studies described, the study should be classified as closely as possible to one of the four listed categories. When in doubt, a higher risk level should be presumed.

2. The affiliation of the person(s) conducting the study should next be categorized in one of three categories:

A. *Research conducted by MDPH workforce (or agents).* This category includes any research projects in which MDPH employees are principal investigators or any research projects that are conducted by one or more people acting as an agent for the MDPH. In this context, an agent of the MDPH is someone who is not an employee of the MDPH but who is acting on behalf of one or more MDPH program offices and is acting at the direction of MDPH staff in conducting the investigation.

B. *Research not conducted by MDPH workforce (or agents) but either funded by MDPH or conducted by an agency that is funded by MDPH*: This category includes research projects that do not fall under the first category, but do involve financing by MDPH. This includes studies in which MDPH provides substantial funding for the study (e.g., greater than 50% of the costs of the study) or studies conducted by an agency which receives substantial funding from MDPH (e.g., greater than 50% of operating costs). This category is intended to include only those studies and/or agencies that are substantially supported by MDPH. It does not include, for instance, federal funds which are distributed via MDPH or other sources of funding which "pass through" MDPH without substantial involvement of the MDPH.

C. *Research not conducted by MDPH workforce (or agents) and not funded by the MDPH*: This category includes all other research projects not covered under categories A or B in which MDPH is not directly or indirectly involved with conducting or funding the study.

3. Using the above two classifications, the appropriate box in RaDAR and IRB Review Determination table listed below should be identified. This box describes the requirements for review by the MDPH HRRC (Human Research Review Committee) or by institutional IRB's, as well as the requirements for RaDAR review for the proposed research study.

A. MDPH HRRC review required means that the project must be submitted to the MDPH HRRC for full or expedited review and approval, as determined

appropriate by the HRRC chairman, as a condition for Commissioner approval under §24A. In some limited cases, MDPH HRRC review may be waived.

B. Institutional IRB review required means that the project must be reviewed and approved by the IRB of the institution that is sponsoring the research. Institutional IRB refers only to non-commercial IRB's that have an assurance of compliance with the Common Rule from the federal Office for Human Research Protection.

C. RaDAR review required means that the researcher must submit an application for § 24A approval to the RaDAR Coordinator. The § 24A application will be combined with § 24B for access to birth records, § 202 for fetal death records, § 111B for cancer registry records, § 24B/67E for birth defects data or other applicable statutes.

		Risk Level			
		Level I - Minimal Risk Study based on existing data only, including: • No contact with human subjects; and • No access to MDPH confidential data; and • Access to non-MDPH confidential data.	**Level II A - Moderate Risk** Study based on existing data only, including: • No contact with human subjects; and • Access to MDPH confidential data.	**Level II B - Moderate Risk** Study based on collection of new data, including: • Contact with human subjects; and • No access to MDPH confidential data; and • Access to non-MDPH confidential data.	**Level III - Highest Risk** Study based on collection of new data, including: • Contact with human subjects; and • Access to MDPH confidential data; or • Any case-control study involving human subject contact; or • Any study involving biological sampling and testing.
Affiliation of Researcher	**Research conducted by MDPH workforce**	RaDAR Committee review required and MDPH HRRC review required	MDPH HRRC review required; and RaDAR Committee review required	MDPH HRRC review required; and RaDAR Committee review required	MDPH HRRC review required; and RaDAR Committee review required
	Research <u>Not</u> conducted by MDPH workforce, but funded by MDPH or conducted by MDPH-funded entity	IRB review required*	MDPH HRRC review required; IRB review required*; and RaDAR Committee review required	MDPH HRRC review required; and IRB review required*	MDPH HRRC review required; IRB review required; and RaDAR Committee review required
	Research <u>Not</u> conducted by MDPH workforce and <u>Not</u> funded by MDPH	No MDPH review required	IRB review required*; and RaDAR Committee review required	No MDPH review required.	MDPH HRRC review required; IRB review required*; and RaDAR Committee review required

* "IRB review required" means the non-MDPH entity must have the research reviewed by the entity's sponsoring IRB.

Procedure Title:	De-Identification, Limited Data Sets, and Aggregate Data		
Procedure Number:	7	**Version #**	2.0
Effective Date:	May 3, 2004		

Content

I. Purpose and Scope

This procedure specifies standards under which individual-level or aggregate data can be disclosed if information that can identify a person has been removed or restricted to a limited data set. This procedure applies to both covered and non-covered components of the Department, and to all Department workforce members, unless otherwise stated.[32] Individual-level data are considered de-identified, provided that they meet the standards established in this procedure; however, a Center retains the discretion not to release data that it believes risks identification of the data subject. Aggregate data release standards may vary among centers and the discretion not to release any particular aggregate data remains with the individual center.

[32] This procedure does not apply to disclosures of unrestricted, identifiable vital record information made by the Registry of Vital Records and Statistics in accordance with applicable laws.

II. Standards for Disclosure of Individual-Level Data

The disclosure of individual-level data containing confidential information may only be made as described in Procedure # 3: Use and Disclosure of Confidential Information. For purposes of this procedure the most relevant categories include:

- Information that is de-identified in accordance with the requirements of section II.A in this procedure. Unless otherwise restricted by law, records de-identified pursuant to this procedure and, where relevant, Procedure # 8: Public Records Release Standards for Documents Containing Medical Information**,** may be made available pursuant to the provisions of the Massachusetts Public Records Law. Information that is defined in statute as confidential or not a public record is not releasable as a public record, even if it meets the standards of the safe harbor method defined below.

  and

- Information that is contained in a limited data set, for which a Limited Data Set Agreement is executed, as described in section II.B.

A. De-Identification Standard

Individual-level data are sufficiently de-identified and do not constitute confidential information if one of the following de-identification methods is satisfied:

1. Statistical De-Identification

A qualified statistician using accepted analytic techniques concludes that the risk is very small that the individual-level data could be used, alone or in combination with other reasonably available information, to identify the subject of that data.

- For purposes of this procedure, a qualified statistician shall mean a member of the MDPH workforce, who is identified by the Center Director for this purpose and approved by the Privacy Office.
- The process for making this determination must be documented in writing and approved by the Privacy Office.
- The documentation shall be maintained with the file including the individual-level data and record of disclosure.

or

2. "Safe Harbor" Method

Individual-level data are considered de-identified under the safe-harbor method if:

a. All of the identifiers listed in this subsection are removed and the Department workforce member who discloses the information de-identified in accordance with this subsection does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information.

b. Identifiers of the individual or of relatives, employers, or household members of the individual that must be removed, including:

- Names;
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes.[33] However, the initial three digits of a zip code may remain in the information if, according to current publicly available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits for all such geographic units containing 20,000 or fewer people is changed to 000;
- All elements of dates (except year) for dates directly relating to an individual, including birth date, dates of admission and discharge from a health care facility, and date of death. For persons age 90 and older, all elements of dates (including year) that would indicate such age must be removed, except that such ages and elements may be aggregated into a single category of "age 90 or older";
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate or license numbers;
- Vehicle identification and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger prints and voiceprints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code, except as permitted under section II.A.3.

3. Re-Identification of De-Identified Data

The Department may assign a code or other means of data identification to allow information that has been de-identified to be re-identified provided that:

[33]For non-covered components, the location of a residential facility including, but not limited to, a hospital, long-term care facility, rest-home, substance abuse facility or other community based facility where an individual temporarily stays or permanently resides shall not be considered identifiable information.

a. The code or other means of data identification is not derived from or related to information about the individual and cannot otherwise be translated to identify the individual; and

b. The Department does not disclose the code or other means of data identification for any other purpose, and does not disclose the mechanism for re-identification.

B. Limited Data Set Standard

A limited data set (LDS) is a mechanism by which individuals or entities outside the Department may apply for access to data that is not entirely de-identified, as described in section II.A for public health purposes or health care operations[34]. If not otherwise restricted by law, the Department may, in its discretion, release certain confidential information in a limited data set provided that:

- The data set meets the standard for content described in section II.B.1.
- The request is reviewed and approved by the Department's RaDAR Committee or a subcommittee of RaDAR charged with LDS review;
- The Center that holds the data enters into a Limited Data Set Agreement with the limited data set recipient;
- All individuals that will have access to the Limited Data Set are identified in the agreement and submit a signed confidentiality agreement to the Department; and
- The LDS is for public health or health care operations and the data are limited to that reasonably necessary to achieve the purposes of the disclosure as specified by the minimum necessary requirements contained in Procedure # 3.

1. Content of Limited Data Sets

a. Identifiers That Must be Removed

A limited data set is confidential information that ***excludes*** the following direct identifiers of the individual, or of relatives, employers or household members of the individual:

- Names;
- Postal address information (street name and number);
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;

[34] Although the HIPAA Privacy Rule provides that a covered entity may disclose a limited data set for the purposes of research, public health, or operations, based on the MDPH Confidentiality Policy and Procedures, the LDS is generally not for use by the Department for research. For research and agreements to use for research see Procedure # 6: Research Requirements.

- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images.

b. Permissible Identifiers

A limited data set ***may*** include the following information:

- Admission, discharge, service and incident dates;
- Dates of birth or death;
- Five-digit zip code or any other geographic subdivision, such as state, county, city, town, precinct, census track, block group and their equivalent geocodes, except for street name and number;
- Unique Identification Codes that allow information that has been de-identified to be re-identified, including those that are derived from or related to information about the individual provided that the mechanism for re-identification is not disclosed; and
- Any other information that is not specified in section II.B.1.a.

2. Required Restrictions on Use and Disclosure of Limited Data Set

The limited data set agreement must:

a. Establish the permitted uses and disclosures of the limited data set by the recipient, consistent with the purposes of public health or health care operations;

b. Limit who can use or receive the data and require a signed confidentiality agreement from each individual who will access the data;

c. Provide that the recipient will:

- Not use or further disclose the information other than as permitted by the Limited Data Set Agreement or as otherwise required by law;
- Use appropriate physical, technical and administrative safeguards to prevent use or disclosure of the limited data set other than as provided for in the Limited Data Set Agreement;
- Report any use or disclosure of information not authorized by the Limited Data Set Agreement to the contact for the Center providing the data and the MDPH Privacy Office.
- Ensure that any agents, including a subcontractor to whom it provides the limited data set, agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information;
- Not attempt to identify any data subject or contact any data subject.

3. **Center Requirements Related to Limited Data Set Agreements**
   - **a.** It is recommended that Centers use the Department's model Limited Data Set Agreement. The agreement constitutes the minimum requirements. Centers may include additional provisions. If Centers use a different agreement, they shall verify that the minimum elements in the model Agreement are included.
   - **b.** All Limited Data Set requests for the release of confidential information must be submitted to and approved by RaDAR, or a subgroup of RaDAR, prior to execution of the LDS Agreement and the disclosure of confidential information. A representative of the Center holding the data requested shall be part of the subgroup reviewing the LDS request. This requirement includes all LDS released by the Department.
   - **c.** The Center that enters into a Limited Data Set Agreement shall maintain a copy of the agreement and shall provide a copy to the RaDAR coordinator.
   - **d.** Department workforce members shall immediately report to the Privacy Office any breach of a Limited Data Set Use Agreement of which they are aware, as described in Procedure # 1: Administrative Requirements. The Department will take reasonable measures to cure the breach, which may include termination of the Limited Data Set Use Agreement and access to the limited data set.

III. Standards for Disclosure of Aggregate Data

A. General Requirements

1. Aggregate data are data collected from individual-level data that have been combined with other individual-level data for statistical or analytical purposes and are maintained in a form that does not permit the identification of individuals. Data that satisfy the aggregate data standards specified in this section are de-identified and constitute a permissible disclosure under Procedure # 3.
2. The aggregate data standards below are a minimum standard. Any Center may adopt more restrictive standards for disclosure of aggregate data. Regardless of whether a Center follows the Department standards specified below or its own more restrictive standards, each Center that discloses aggregate data must ensure that there is no reasonable basis to believe that any identifying information could be derived from disclosure of the aggregate data. When multiple data sets are used, the standard for the data set with the most restrictive rules must be followed. When utilizing data from other agencies, workforce members using the data are responsible for complying with the standard for aggregate data release for that agency and to insure that it is followed, if it is more restrictive than the MDPH standard.
3. Each Center privacy liaison shall document and provide to the Privacy Office the aggregate data release standard or standards adopted by the Center.

4. All MDPH publications (all public releases including publications and web releases) containing aggregate data shall be reviewed through the MDPH Peer Review Process or a comparable committee or process to verify that the Department or Center aggregate data release standard is met prior to release.

B. De-identification Methods for Covered Components

Covered components may utilize either of the two methods listed in this subsection for ensuring that aggregate data meet the de-identification standard. The criteria specified below are minimum standards for disclosure of aggregate level data.

1. Statistical De-Identification

A qualified statistician using accepted analytic techniques concludes that the risk is very small that the aggregated information could be used, alone or in combination with other reasonably available information, to identify the subject(s) of that data.

- For purposes of this procedure, a qualified statistician shall mean a member of the MDPH workforce, who is identified by the Center Director for this purpose and approved by the Privacy Office.
- The process for making this determination must be documented in writing and approved by the Privacy Office.
- The documentation shall be maintained with the files related to the aggregate data released.

or

2. "Safe Harbor" Method

The aggregate data do not contain any of the 18 identifiers listed in section II.A.2

C. De-identification Methods for Non-Covered Components Only

In addition to either of the methods for covered components listed in section III.B, non-covered components may utilize one of the following three additional methods for ensuring that aggregate data meet the de-identification standard.

In determining the appropriate de-identification method for aggregate data, it is strongly recommended that if centers cannot meet the safe harbor standard for aggregate data releases for geographic subdivisions smaller than the state, that they give priority to the standards in sections III.C.1 and III.C.2 listed below. The statistical de-identification method by a qualified statistician should only be applied if the safe harbor and methods described in sections III.C.1 and III.C.2 listed below not viable options.

1. Numerator/Denominator-Based Suppression

Cell sizes based on a combination of denominator[3] (population from which the health events arise) and numerator[4] (health event) are suppressed in accordance with the table below.[5] Aggregate data with denominator and numerator values greater than those indicated in the table may be considered sufficiently de-identified so as not to constitute confidential information, and may be disclosed.

DENOMINATOR (D)	NUMERATOR (N)	STANDARD
10-29	1-4	Suppress numerator and any other cells[6] that would allow for the calculation of any other cells with values of 1-4
10-29	5-29	Suppress any cells that would allow for the calculation of any other cells[6] with values of 1-4
0-9	0-9	Suppress numerator
= N	= D	Suppress numerator unless privacy risk is minimal

2. Numerator Based Cell Suppression

- Suppress all statistical cells with one to five subjects; and
- Suppress all statistical cells that would allow for the calculation of any other cells with values of 1-4.[6]

or

3. Alternative Suppression Standards

Any Center may develop an alternative aggregate data release standard if it decides not to follow any of the standards above, provided that:

- The standard is at least as restrictive as the above stated standards; and

[3] Population or denominator means: For counts of health events (cases, diagnoses, births, discharges, etc.), the population or denominator is defined as the number of people who live in a particular community, are clients of a particular program, or patients in a particular facility. The population or denominator may be further delineated by demographic information (e.g., race, age, gender, etc.). For additional cross-classifications, the denominator is defined as the number of events or the numerator for the preceding cross-classification or the population

[4] Numerator means: The number health events (cases, diagnoses, clients, discharges, encounters, visits, etc.) being considered for release for a particular population or cross-classification.

[5] For additional guidance and examples for applying numerator/denominator-based suppression, see *Department of Public Health Aggregate Data Release Guidelines*.

[6] Because it is possible to figure out a suppressed value from column and row totals when only one value is suppressed, it may also be necessary to either suppress the column and row totals or suppress other cells so that no column or row has only one suppressed value.

- Any alternative standard is documented by the Center and approved by the Privacy Officer prior to implementation.

Authority: M.G.L. c. 66A
45 C.F.R. §164.514

Forms: Limited Data Set Agreement

Procedure Title:	Public Records Release Standards for Documents Containing Medical Information		
Procedure Number:	8	**Version #**	2.0
Effective Date:	May 3, 2004		

Content

I. Purpose and Scope

This procedure describes how to protect the privacy of individuals whose medical information is contained in DPH reports and documents requested as public records.

This procedure applies to all documents containing medical files or medical information [hereinafter referenced as medical information] including, but not limited to, Statements of Deficiencies (SOD), complaint and incident investigation reports, licensure or inspection reports, external review documents, and records relating to disease investigations. All Department workforce members, in both covered and non-covered components of the Department, must comply with this procedure.

II. General Requirements

Before releasing any reports and documents containing medical information pursuant to a public records request, workforce members should engage in the following process:

A. Determine if the requested materials contain any one of the following three categories of information:
- Direct identifiers;
- Medical information related to an individual; or
- Indirect identifiers.

B. Redact or withhold any information falling within one of the three categories; and

C. Release the materials as a public record unless another Public Records Law exemption prohibits the release.

III. Redaction Standards Applicable to all Documents

The standards for redacting identifiers and medical information under this section apply to all Department documents and reports. As discussed in section IV, programs are responsible for developing standards for redacting indirect identifiers specific to program needs.

A. Direct Identifiers

Workforce members shall redact all direct personal identifiers from all documents that include medical information prior to public release including, but not limited to:

1. All names[35] of individuals who received medical care, resided in the facility, or filed a complaint;[36]
2. All dates directly related to an individual. Centers shall redact the day and month (but may include the year) for the following dates:
   - Admission date;
   - Discharge date;
   - Date of incident;
   - Date of service;
   - Date of birth;[37] and
   - Date of death.
3. The home address (including street, town, county, state, country, and zip code) and phone number of any individual included in the document. This does not include the address of a residential facility including, but not limited to, a hospital, long-term care facility, rest-home, substance abuse facility or other community-based facility; and
4. All personal identification numbers including a social security number; medical record number; and health plan number.

B. Medical Information

Centers shall not release any medical information that relates to an individual, with the exception of the general medical condition or category of complaint that some programs may determine is necessary to retain, as described in section IV.

Medical information is not necessarily physically located in a single "file," and turns on the nature or character of the documents and not the label or location of the documents. This includes medical information lacking direct identifiers that could be used to identify an individual,[38] as opposed to aggregate medical information[39] from more than one individual's file.

---

[35] To the extent that reports are drafted with a generic reference (i.e., patient A) rather than an individual name, no redaction for this item would be required.

[36] Exemption (f) of the Public Records Law (M.G.L. c. 4, §7(26)) permits the agency to withhold the name of the complainant, without having to show prejudice to an ongoing investigation.

[37] In unusual circumstances, the year of birth should be redacted if its inclusion risks identifying an individual.

[38] The release of medical information, even without other particular identifying details creates a serious risk of identification by those who are familiar with the individual. The risk of identification is enhanced in

Medical information includes the nature and extent of a person's medical condition. This includes medical statements, for example, such as a bad back, heart problems and hypertension if related to a specific person. It also includes autopsies and blood tests, as well as information that is diagnostic in nature and that yields detailed, intimate information about the subject's body and medical condition.

C. Medical Records and Abstracts

Medical records and abstracts are a subset of medical information. A medical record is an independent document created by the provider as part of providing health care, which a Center is given or collects in the process of its oversight functions. Medical abstracts are also independent documents, created by a DPH investigator from the medical record and include only medical information taken directly from the medical records of a provider. Medical records and abstracts are wholly exempt from release.

D. Non-Segregable Materials

Sections of reports or documents containing non-segregable medical information may be redacted in their entirely. Material is considered non-segregable if redacting the medical information from the section leaves information with no independent meaning. For example, the redaction of the medical information in a section of a document might leave only conjunctions such as “and” “but” and “or.” This section should be redacted in its entirety because the string of conjunctions has no independent meaning.

IV. Program-Specific Redaction Standards[40]

A. Indirect Identifiers

Indirect identifiers are elements in documents and records which implicate privacy interests by increasing the likelihood of identifying an individual, but do not involve direct identifiers or medical information.

The indirect identifiers left in any specific document may vary from program to program and depend on whether the indirect identifier serves to increase the likelihood of identifying the individual and whether the privacy interest of the individual outweighs the public interest in releasing the indirect identifier. For

---

those instances that relate to surveys, inspections, complaints or investigations of particular licensed, identified facilities at a particular point in time. Moreover, the ability to link information electronically and to tie it to other information in the public domain has greatly increased the risk of identifying individuals from limited information.

[39] Release of aggregate information must comply with Procedure # 7: De-Identification, Limited Data Sets, and Aggregate Data.

[40] It is recommended that these redaction standards be set at the program level, as they are likely to differ from program to program within a Center.

example, Health Care Quality (HCQ) will release the name of the facility in a hospital or nursing home inspection report since the performance of the facility is precisely what is at issue in the report, the likelihood of increasing the chance of identifying the individual is limited, and there is a strong public interest in its release. On the other hand, the Office of Patient Protection (OPP) will redact references to a specific facility, but not to the health plan, since it is the health plan and not the facility that is at issue in the matter on appeal. Moreover, the name of a facility coupled with the health plan could serve to identify the individual in an OPP decision and therefore, should be redacted.

Each program that releases such documents as public records shall formulate its own protocol for redaction of indirect identifiers commonly found in their documents including, but not limited to:

- The name of a facility, provided that it is not the subject of the incident, investigation or case in review;
- The name(s) of medical provider(s), employee(s) of the facility or a witness(es) to events provided that they are not the subject of the incident, investigation or case in review;
- Age of individual: exact age, age range, or age category (i.e. adult, child, infant);
- General medical condition or subject of incident, investigation or case in review. (e.g., OPP may release a decision that states that the appeal relates to a denial of coverage for a breast reduction. HCQ may identify the category of complaints as those relating to gastric by-pass surgery. The inclusion of this information is necessary to identify the incident, investigation or case in review. No other medical information should be included); and,
- Other personal information (e.g., marital status; paternity; government assistance; family disputes; and reputation).

B. Report Writing Considerations

Each Center[41] should review this procedure and the protocol developed pursuant to this procedure to determine, to the extent possible, how to modify its report writing requirements to accommodate these standards without the need for redaction. If certain information, which must be redacted prior to public release, is required to be included in the reports/documents, programs should set standards for writing and formatting the reports to ensure their readability.

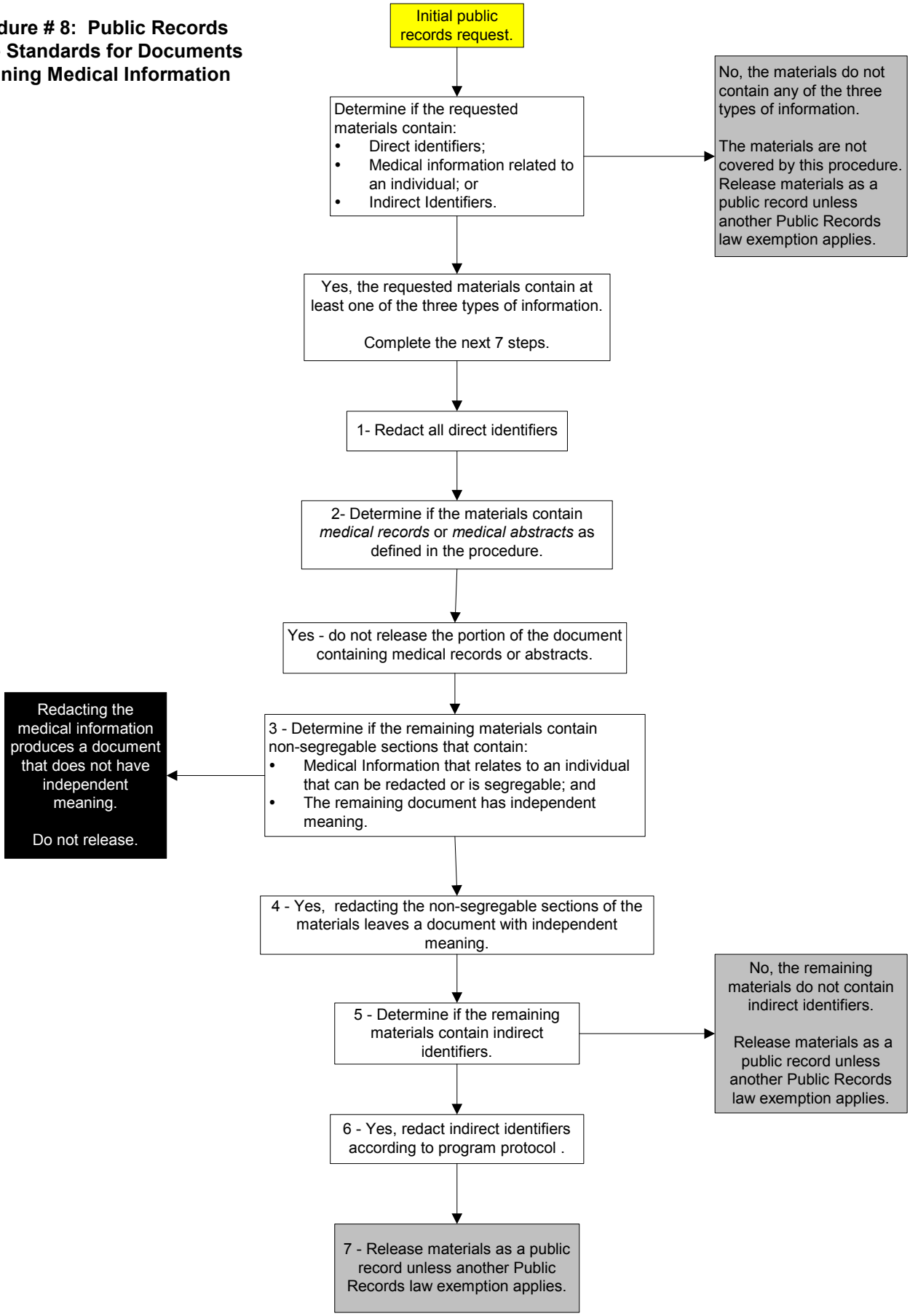
Each Center should also review its report writing requirements and decide whether to add a summary of the report, either as an executive summary or a separate document, which includes no identifiers or medical information. This may be particularly important if the program deems it necessary to provide a context for its findings or to provide the public with sufficient information to fulfill its health oversight

[41] These considerations should be coordinated at a Center level, but again may differ from program to program.

functions. The decision to issue a summary is within the discretion of the Department and shall be made by the Center director or designee.

Authority: M.G.L. c. 4, § 7(26) and M.G.L. c. 66A
45 C.F.R. § 164.514

Procedure # 8: Public Records Release Standards for Documents Containing Medical Information



Procedure Title:	Verification of Individuals or Entities Requesting Disclosure of Confidential Information		
Procedure Number:	9	**Version #**	2.0
Effective Date:	May 3, 2004		

Content

I. Purpose and Scope

This procedure describes generally how to determine whether the Department is permitted to release confidential information to the individual or entity making the request. Centers should use this procedure as guidance; however, each Center should create program-specific procedures for verification that more closely relate to the information maintained by the Center. This procedure applies to both covered and non-covered components of the Department and all Department workforce members.

II. General Requirements

Prior to disclosing confidential information Department workforce members should generally follow a four-step process:

A. Classify the type of requestor (i.e., data subject requesting their own confidential information; an employee of another state agency);
B. Verify the authority of the individual or entity to receive access to the confidential information they have requested as discussed in section III;
C. Verify the identity of the individual or entity requesting access to the information; and
D. Verify the records requested as discussed in section IV.

III. Verification of the Requestor's Authority

First, determine whether the individual or entity requesting the disclosure of confidential information is permitted to have access to the information. The best method for determining this is by considering whether the disclosure is permissible under Procedure # 3: Use and Disclosure of Confidential Information. For example, consider whether:

- The request is from the data subject for his or her own confidential information;
- The request is from the data subject's personal representative for the data subject's confidential information, and is accompanied by the appropriate documentation;
- The request is accompanied by an authorization and the authorization meets the requirements of Procedure # 4: Authorizations for the Use and Disclosure of Confidential Information;
- The request is from a government agency authorized to receive the disclosure for public health purposes;
- The request is for confidential information for a research study approved by the Commissioner pursuant to M.G.L. c. 111, § 24A and meets the requirements of Procedure # 6: Research Requirements; or,
- The request is pursuant to a subpoena or court order, and meets the requirements of Procedure # 5: Responding to Subpoenas.

IV. Verification of the Record Requested

After determining that the disclosure is permitted and verifying the identity of the requestor, workforce members must take steps to verify that the record requested is the appropriate record. Each program may differ in the steps required for such verification, depending on the type of information held by the program with respect to the individual's served by the program. Among the items that may be used to verify the record are full name, social security number, date of birth, address at the time of service, any other personal identifiers, or name of parents or guardian.

The chart below provides guidance on the steps in the verification process; however, each Center or program should develop its own procedures in this area.

Authority: M.G.L. c. 66A
45 C.F.R. §§ 164.504(g) and 164.514(h)

Classify the Requestor	Verify Requestor's Authority	Verify Requestor 's Identity	Verify Records
The data subject (DS)	None required	In person Requests: Ask for a picture ID or two other forms of identification if you are not familiar with the individual from prior experience. Request by mail, fax or telephone: Verify address or fax or phone number using Department records or independent sources.	Request that the DS provide sufficient information to show that these are his or her record, including: • Full name • SSN • Date of Birth • Address at the time of service • Any other personal identifier used by program • Name of parents or guardian
The representative of the DS: • Parent of the minor • Legal guardian • Health-care proxy • Executor or Administrator of DS's estate • Conservator • Durable Power of Attorney	Locate records and determine whether the records contain the below listed documents. If not, they must be submitted before proceeding. Records include legal documentation designating individual as the DS's representative. or The DS is a minor and the requestor is listed on the records as the parent of the minor. Check with OGC if you have question about what documentation is required or the sufficiency of the documentation.	Same as above And Requests by mail: Request on official or business letterhead, if applicable.	Request that the individual provide sufficient information to show that he or she is receiving the appropriate record, including: • Full name of the DS • SSN of DS • Date of birth of DS • Address of DS at time of service • Any other personal identifier for DS • Name of parents or guardian
The spouse, relative, friend, or other person identified by the DS. or A legislator	None required. It is the same as the DS above. Since the DS is present and gives verbal consent for MDPH to speak to the other individual and indicates the scope of the information, it is okay to disclose information to the other person. This can only be done in person or by telephone, with the DS present. The DS does not have to stay on the phone, once he or she gives the consent.	Verify the identity of the DS in the same manner that you would if the DS was alone. It is not necessary to verify the identity of the other person identified by the DS. You should note the name of the other person in the file. In person Requests: Ask for a picture ID or two other forms of identification if you are not familiar with the DS from prior experience. Request by telephone: Verify phone number using Department records or independent sources.	Request that the individual provide sufficient information to show that he or she is receiving the appropriate records, including: • Full name of DS • SSN of DS • Date of birth of DS • Address of DS at time or service • Any other personal identifier for DS • Name of parents or guardian

Classify the Requestor	Verify Requestor's Authority	Verify Requestor 's Identity	Verify Records
The spouse, relative, friend, or other person identified by the DS or A legislator	If the DS is not present to confirm the requestor's authority, then a written authorization in compliance with Procedure #4 is required.	<u>In person Requests</u>: Ask for a picture ID or two other forms of identification if you are not familiar with the individual from prior experience. Government ID badge or request on official letterhead if the official is not known based on prior experience. <u>Request by mail, fax or telephone</u>: Verify address or fax or phone number using Department records or independent sources. Request on official or business letterhead, if applicable	Assure that the written authorization provides sufficient information to show that the information on the records relates to the information provided on the authorization form, including the elements listed above.
A MDPH employee who needs the information to perform his or her duties	Verify that the program is authorized under Procedure #3 to use such information • Intra-Departmental Data Use Agreement • Agreement for Research issued by RaDAR • DS authorization or consent *And* Verify that the workforce member is authorized to use such information (role based access).	MDPH ID badge if you are not familiar with the individual from prior experience. Letter from MDPH Center/Bureau or program Director authorizing the individual workforce member (fulfills role based access requirement)	Refer above to the elements identified, unless the request includes the entire data base. Verify the data base against the data use agreement.
An employee of another state agency who needs the information to perform his or her duties	Verify that the Agency is authorized under Procedure #3 to have the information disclosed. • Inter-Departmental Data Use Agreement • Agreement for Research issued by RaDAR • DS Authorization *And* Verify that the requesting employee is authorized to access such information.	Verify that the individual is an employee of the requesting agency. Check for agency ID badge or other official credential including a specific request on agency letterhead if you are not familiar with the individual from prior experience.	Refer above to the elements identified unless the request includes the entire data base. Verify the data base against the data use agreement.
A MDPH vendor who contracts with MDPH to provide services	Verify that the Vendor is authorized under Procedure #3 to have the information disclosed; that the records requested relate to the services for which the vendor contracts with MDPH; and that the individual is authorized by vendor to receive such information. • Contract • DS authorization	Verify that the individual is an employee of the requesting entity through employee identification badge or a specific request on the vendor's letterhead if you are not familiar with the individual from prior experience.	Refer above to the elements identified unless the request includes an entire data base. Verify the data base against the data use agreement.

Procedure Title:	Security of Confidential Information		
Procedure Number:	10	**Version #**	2.0
Effective Date:	May 3, 2004		

Content

I. Purpose and Scope

This procedure describes the standards for ensuring the security of the confidential information collected, maintained, used and disclosed by the Department. This Procedure applies to both covered and non-covered components of the Department, and all Department workforce members.

II. Transmission of Confidential Information

Department workforce members must take steps to ensure the security of confidential information transmitted within the Department, and to non-DPH entities. Workforce members shall disclose confidential information only when the disclosure is permissible under Procedure # 3: Use and Disclosure of Confidential Information.

A. Disclosures Made by U.S. Mail

When sending confidential information by U.S. mail workforce members must:

1. Send the information in a security envelope marked “Confidential”;
2. Include their name and a return address;

3. Verify that the recipient's address is correct as described in Procedure # 9: Verification of Individuals or Entities Requesting Disclosure of Confidential Information; and
4. Send the information by registered or certified mail, or another method that provides delivery tracking, whenever feasible.

B. Disclosures Made by Delivery or Courier Service

When sending confidential information by hand delivery or courier service, workforce members must:

1. Verify the name and address of the intended recipient as described in Procedure # 9;
2. Seal the information under protective cover (e.g., a folder or envelope) and mark the package "Confidential";
3. Use a reputable courier service known to the Department;
4. Verify the identity of the individual who will be delivering the package as described in Procedure # 9. Workforce members should also record the courier's name, time of pick-up, and other identifying information (such as employee number) available from the identification presented by the courier; and
5. Retain a tracking number, and the intended recipient informs you that the information was not received, contact the delivery service to track the item, if applicable.

C. Faxing Confidential Information

1. Confidential information should be hand delivered or mailed whenever feasible. Faxing of confidential information is allowable in situations when information is needed immediately, or when mail or courier delivery will not meet a necessary timeframe.
2. Faxed confidential information must only be sent to, or received at, secure/confidential locations. Confidential information should never be sent to unsecured fax machines such as those located in unmonitored or high-traffic areas, or where unauthorized individuals can search through incoming faxes.
3. Centers shall take steps to secure fax machines used to send confidential information. Examples of appropriate efforts include:
    - Move fax machines from areas open to the public/non-authorized personnel to areas where only authorized personnel have access;
    - Establish fax numbers to be used only for faxing confidential information, which will be accessed only by authorized personnel; and
    - Designate an authorized individual(s) to be responsible for retrieving and sending faxes containing confidential information. In addition, train workforce members not to sort through faxes.

4. When transmitting confidential information by fax, workforce members must:
   a. Verify the identity of the recipient and their fax number as described in Procedure # 9.
   b. Call to notify the recipient that a fax containing confidential information is being sent. Ask the recipient to attend the fax machine until transmittal is complete, unless it is known that the receiving fax machine is in a secure, limited-access location, or the receiver uses a desktop fax application.
   c. Request that the recipient confirm receipt of the fax. If the recipient does not confirm receipt within a reasonable period of time, call the recipient to confirm receipt.
   d. Use either MDPH's standard fax cover sheet or a Center-specific cover sheet that contains:
      - A confidentiality statement; and
      - Instructions directing the unauthorized recipient of a misdirected fax to contact the sender. Also, in the event of a misdirected fax, the unauthorized recipient should be directed to immediately destroy the fax or return the information to the sender, as directed by the sender.
   e. Activate the fax confirmation option if available, and verify transmission with fax activity confirmation sheet.
   f. Remove the faxed documents from the vicinity of the fax machine, including the fax activity confirmation sheet after transmission. Keep fax activity confirmation sheets with original documents.
   g. Remove all documents containing confidential information from the vicinity of the fax machine before contacting the intended recipient when there is a problem with an attempted transmission.

D. Disclosures Made by Telephone

When transmitting confidential information by telephone, workforce members must take the following steps:

1. Verify the identity of all requestor's seeking the disclosure of confidential information over the telephone, as discussed in Procedure # 9.
2. Disclose confidential information by telephone only from a secure or private area whenever feasible. The use of cellular phones or public telephones to communicate confidential information should be avoided.
3. Never leave messages with confidential information on voicemail, answering machines or with individuals other than the data subject or their personal representative. Information left in messages shall be generic in nature and not indicate services being performed or provider of such services, unless the data subject has directly requested otherwise. Such requests should be documented and maintained by the Center receiving the request.

E. Restrictions on Email and Email Attachments

No confidential information shall be transmitted by email or email attachment unless by means of a Departmental approved secure system. Contact the Privacy Office for more information.

III. Storage of Confidential Information

Confidential information shall be stored and maintained by the data custodian in a manner that protects the confidentiality, integrity and availability of the information. Access to the confidential information must meets the Department's minimum necessary and role-based access standards as described in Procedure # 3. Workforce members shall not remove confidential information from the work site including paper or electronic information, unless it is required for a field visit, meeting or otherwise necessary for work related purposes and only if pursuant to Center procedures. Appropriate measures shall be taken in each instance to insure that confidential information removed from the building is secured from unauthorized access.

A. Paper-Based Confidential Information

Improper storage of on-site paper-based files may result in the improper disclosure of or access to confidential information, including the storage of files in unlocked file cabinets. Centers shall take steps to secure paper-based confidential information, including:

1. Move confidential information to locked file or purchase and install locks on existing non-locked cabinets;
2. Move file cabinets or other storage sites from "public" areas to low-traffic areas;
3. Move workforce members and storage so that those workforce members who need access to the materials are located near the storage area, and those not requiring access are relocated away from the area; and
4. Move file cabinets without locks into rooms that can be locked or otherwise secured, and limit access to rooms with unlocked cabinets based on a need to know/role-based access.

B. Printers and Copiers

Improper disclosures of confidential information can occur through the use of unsecured printers and copiers. Examples of unsecured printers or copiers are printers or copiers located in unmonitored or high-traffic areas that allow unauthorized individuals to search through documents left at the printer or copier. Centers shall take steps to secure printers and copiers, including:

1. Move printers to enclosed areas to which only authorized personnel have access;
2. Designate separate/dedicated printers and copiers to be used only for printing and copying confidential information; and
3. Train staff to immediately retrieve papers that contain confidential information from printers and copy machines.

C. Electronic Confidential Information

1. Electronic confidential information shall be maintained by the data custodian in a manner that protects the confidentiality, integrity and availability of the information.
2. A computer from which confidential information is accessed must be password protected or in a secure area.
3. Workforce members are responsible for complying with the Information Technology Security standards and guidelines listed in Appendix A.
4. Workforce member's access rights must meet the Department's role-based access and minimum necessary standards as described in Procedure # 3. Workforce members shall not circumvent prescribed access rights by sharing their passwords, or utilizing another workforce member's password to access confidential information beyond the scope of their authority to access.

a. Terminated Employees

IT Services must be immediately notified when workforce members are terminated so that the workforce member's access rights can be terminated immediately.

b. Transferring and Resigning Employees

Program management, Human Resources, and IT Services should coordinate the date and time of a workforce member's transfer or resignation so that computer network access is altered or terminated as required under the circumstances.

IV. Disposal of Confidential Information

Confidential information that is no longer needed shall be destroyed whenever possible, or archived, consistent with the Center's record retention policies and the requirements of the Records Conservation Board.[42]

A. Paper-Based Records

The proper destruction of paper-based confidential information before disposal is the primary means of ensuring its confidentiality. Centers shall take steps to ensure the proper destruction of paper-based confidential information before disposal, including:

- Purchase shredders and place them near recycling and garbage bins; and
- Purchase secure bins with locked tops, and contract with vendors to ensure secure disposal.

[42] Information related to the Massachusetts Records Conservation Board is available at http://www.state.ma.us/sec/arc/arcrcb/rcbidx.htm.

B. Electronic Records and Files

Confidential information stored on electronic media (e.g., disk, CD, etc.) shall be completely erased before disposal.

Authority: M.G.L. c. 66A § 2
45 C.F.R. § 164.530(c)

Massachusetts Department of Public Health
Confidentiality Policy and Procedures
Appendix: MDPH IT Security Standards

The latest version of the Department's Information Technology standards and guidelines can be found at http://healthnet/services/ITS/index.htm.

1. *MDPH Acceptable Use Policies* (Effective Date: 7/01/02)
These policies cover the use of, and access to, computers, Local Area Networks (LANS), Wide Area Networks (WANS), electronic mail, the Internet, and voice mail systems at the Department of Public Health. They apply to all MDPH contractors, permanent MDPH employees, and vendor personnel authorized by the Department of Public Health to use any of these resources. Failure to observe these policies may subject an individual to disciplinary action, including termination of a workforce member's employment or contract with the Department.

2. *MDPH Email Address Book Standard* (Effective Date: TBD)
The *Email Address Book Standard* prevents the inadvertent mis-addressing of email by establishing the DPH Recipients Container as the default address book in Outlook for all workforce members. Centers and Bureaus may establish a more restrictive default address book, requiring workforce members to use a specific Center or Bureau-based address book rather than the DPH Recipients Container.

3. *MDPH Screen Lock-Out Standard* (Effective Date: TBD)
The *Screen Lock-Out Standard* establishes a common policy for protecting against unauthorized access to the network, its resources and any confidential information maintained on or accessible by attended or unattended workstations. All DPH workforce members shall use a password-protected screen lock-out which automatically starts after fifteen (15) minutes of inactivity on a workstation. The standard allows Centers to either establish more restrictive settings, or to remove the screen lock-out for public-access workstations provided the available functionality is strictly limited and locked down.

4. *MDPH Confidential Data Encryption Standard*. (Effective May 5, 2001)
The *Confidential Data Encryption Standard* defines the Department's standard as it pertains to protecting sensitive, identifiable information from tampering or inadvertent or malicious disclosure. This includes prohibitions on transmitting confidential information by email and email attachment.

Procedure Title:	Individual Rights Related to Confidential Information		
Procedure Number:	11	**Version #**	2.0
Effective Date:	May 3, 2004		

Content

I. Purpose and Scope

This procedure describes the rights of data subjects[43] relating to the confidential information collected, used and disclosed by the Department. These include the right to request:

- Access to confidential information;
- Amendment of confidential information;
- Communication with the Department through alternative means; and
- Restrictions on the use and disclosure of confidential information.

This procedure applies to both covered and non-covered components of the Department and all Department workforce members. As described below, there are certain limitations on these rights imposed by state and federal laws as well as certain requirements that relate only to covered components.

II. Access to Confidential Health Information

Generally, the Department must inform a requesting data subject if it maintains any confidential information relating to the data subject, and must subsequently make the confidential information available to the data subject. As described in section II.C below, the right of access is restricted in limited situations.

A. Request in Writing

A data subject's request for access must be made in writing, preferably using the form *Request for Access to Confidential Information*.[44] The request must:

[43] All rights in this procedure may be exercised by a data subject's personal representative, provided that the personal representative is authorized for that purpose, as described in Procedure # 9: Verification of Individuals or Entities Requesting Access to Confidential Information.

1. Provide sufficient information to identify the information sought;
2. Specify whether the data subject wants either to inspect or receive a copy of their confidential information; and
3. The data subject's contact information.

B. Granting Access

1. Unless access is restricted as described in section II.2, MDPH must provide the data subject with access to confidential information in:
   - The form or format requested if it can be produced in such form or format;
   - A readable hard copy or other form or format as mutually agreed to by MDPH and the data subject; or
   - A summary of the requested information instead of the actual information if the data subject agrees in advance to the summary and to any fees associated with the summary.
2. The Center may discuss with the data subject the scope, format, time and location for review, and other aspects of the request to facilitate access.
3. Only one copy is required if the same information is maintained in more than one place.
4. The identity of the data subject must be verified prior to granting access, as described in Procedure # 9: Verification of Individuals or Entities Requesting Confidential Information.
5. When providing the data subject access to his or her confidential information MDPH shall remove personal identifiers relating to third-parties, except where a third-party is an officer or employee of government acting in an official role.

C. Denying Access

1. Notice

If access to confidential information is denied in whole, or in part, MDPH will provide the data subject:

a. Access to any other confidential information that is not subject to the exceptions to access listed in section II.2;
b. A timely written denial including the basis for the denial; and
c. A statement of the data subject's right for review of the denial as described in section II.C.3.

2. Grounds for Denying Access

A data subject shall be denied access to confidential information in the following circumstances:

a. Information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding. This information may be withheld until the holder completes its investigation and commences an

[44] As is discussed in section below, versions of the forms referenced in this procedure are at http://healthnet/privsec/forms.htm.

administrative or judicial proceeding, or for one year from the commencement of the investigation, whichever is first.

b. When access to confidential information is restricted by law, including but not limited to information subject to the Clinical Laboratory Improvements Amendments of 1988 (CLIA), and confidential statistical birth information.

c. Confidential information contained in psychotherapy notes.

d. Confidential information created or obtained by MDPH in the course of research currently in progress, provided that:

- The data subject agreed to the temporary denial of access when consenting to participate in the research that includes treatment; and
- MDPH informed the data subject that the right of access will be reinstated upon completion of research.

e. When a licensed health care professional determines in the exercise of professional judgment that the requested access is:

- Reasonably likely to endanger the life or physical safety of the data subject or another individual; or
- Reasonably likely to cause substantial harm to the data subject or another individual.

3. Right of Review

The MDPH Privacy Office will process a data subject's request for a review. If the denial was based on any reason other than a restriction by statue, the request for review of the denial of access will be assigned to a MDPH manager who did not participate in the decision under review.

III. Amendment of Confidential Information

A data subject has the right to request that MDPH amend his or her confidential information maintained by the Department, if the data subject believes the information is incorrect or incomplete. MDPH may deny a requested amendment for the reasons described in section III.C.2. In addition, the right to request amendment of confidential information does not apply to the amendment of any personal data for which the process for amendment is established in statute or regulation. For covered components this also includes the right to amend confidential information held by a business associate.

A. Request in Writing

Requests must be made in writing, preferably using the form *Request for Amendment of Confidential Information*. The request must include:

1. Sufficient information to identify the requested amendment;
2. The reason(s) to support the amendment;
3. Any individuals or entities identified by the data subject as having a need to know of the amendment; and
4. The data subject's contact information.

B. Granting an Amendment

1. If there is no disagreement about the requested amendment, a signed and dated notation will be made in the appropriate file. The amendment form should also be attached to the information that was amended. Centers may develop alternative means of recording amendments to confidential information for both electronic and paper-based records.
2. A copy of the completed amendment response form will be sent to:
   - **a.** The data subject, indicating that an amendment was made;
   - **b.** Individuals identified by the data subject as having a need to know; and
   - **c.** Any others who reasonably can be identified as having received the confidential information, including business associates of covered components, that may have relied or may rely on the information to the detriment of the data subject.

C. Denying the Amendment

1. Notice

MDPH may deny a requested amendment for the reasons described in section III.C.2. If the amendment is denied, MDPH must provide the data subject with a timely written denial including:

- **a.** The basis for the denial;
- **b.** A statement that the request for amendment will be included in any subsequent disclosure of the disputed information;
- **c.** The data subject's right to submit a written statement disagreeing with the denial and a description of how a statement may be filed; and
- **d.** A statement that the data subject's disagreement, along with any MDPH rebuttal, will be included in any subsequent disclosure of the disputed information. Any rebuttal will be provided to the data subject.

2. Grounds for Denial

Acceptable reasons for denying a requested amendment include:

- **a.** The information was not created by the Department;
- **b.** The information is subject to specific amendment procedures pursuant to statute or regulation;
- **c.** The information is not part of the data subject's record as maintained by MDPH;
- **d.** The information is not available for inspection pursuant to MDPH's policy regarding access; or
- **e.** The information is accurate and complete.

D. Amendment of Confidential Information by Non-MDPH Entities

A Center that is informed by another entity about an amendment to confidential information held by, but not created by the Center, shall amend the information by, at a minimum, identifying the affected records and appending or otherwise providing a link to the location of the amendment.

IV. Communications by Alternate Means

A data subject has the right to request that he or she receive correspondence from the Department at an address, telephone number, or by means other than those associated with the subject's home address.

A. Request in Writing

The request must be made in writing, preferably using the *form Request for Alternative Means of Communications*. While a Center shall not require an explanation, the data subject must identify:

1. The specific communications for which the data subject is making the request;
2. A clear alternative means of communication; and
3. The data subject's contact information.

B. Granting or Denying the Request

1. MDPH is not required to agree to communicate by the requested means; however all reasonable requests should be granted. In making this determination, Centers may consider, for example, the expense and administrative burden involved with compliance and whether the alternative means is sufficiently effective in communicating with the data subject.
2. If the request is granted, the Center will notify the data subject that the alternate address and/or telephone number will be used for the specified communications between MDPH and the data subject. The alternate address and/or telephone number will remain in place until changed by the data subject.
3. The Center granting the request must clearly identify the alternative means of communication on the individual's record(s), whether it is paper or electronic.
4. The Center must also provide notice of the data subject's alternate means of communication to the billing department and/or any other departments, providers, and for covered components -- business associates, who may be sending communications on behalf of the Center.
5. If the request is denied, the Center making the determination should send the denial to the alternative means of communication that was requested. The data subject should be informed that all future communications will be directed to the previously listed means of communication.

V. Restrictions on the Use and Disclosure of Confidential Information

A data subject has the right to request restrictions on the use and disclosure of his or her confidential information. However, such a restriction does <u>not</u> restrict the following uses or disclosures:

- To the data subject;
- Those otherwise permitted or required by law;
- For public health activities; and
- for health oversight activities.

A. Request in Writing

All requests must be made in writing, preferably using the form *Request for Restrictions on Use and Disclosures of Confidential Information*. The request must identify:

1. The data subject and the specific confidential information to be restricted;
2. To whom the restriction applies; and
3. The data subject's contact information.

B. Granting or Denying the Request

MDPH is not required to agree to a restriction. Centers should consider whether the request is reasonable. In making this determination, Centers may consider, for example, the expense and administrative burden involved with compliance. If the Center disagrees with the request for restriction, the data subject shall be notified in writing. If a Center agrees with the request for a restriction, it agrees to the following:

1. MDPH may not use or disclose confidential information in violation of the restriction, except to a health care provider when the individual who requested the restriction is in need of emergency treatment and the restricted confidential information is needed to provide the emergency treatment.
2. If restricted confidential information is disclosed to a health care provider for emergency treatment, MDPH must request that such health care provider not further use or disclose the information.
3. The subject of the confidential information must be given notice of such access upon termination of the emergency.

C. Terminating a Restriction

A restriction on use and disclosure of confidential information may be terminated if:

1. The data subject agrees to or requests the termination in writing;
2. The data subject orally agrees to the termination and it is documented; or
3. MDPH informs the data subject that it is terminating its agreement to a restriction and the termination is effective with respect to protected health information created or received after the individual is informed.

VI. Center Requirements: Administration and Documentation

A. Designations and Procedures

Each Center must designate an individual(s) responsible for receiving and processing requests related to data subjects' individual rights. Centers must also develop internal procedures to comply with the requirements of this procedure.

B. Submission and Coordination of Requests

1. All individual rights requests must be made to the Center maintaining the data subject's confidential information. All Centers must keep a log of all requests for individual rights made under this procedure.

2. All responses to requests should be made on the back of a copy of the original request, or on a page attached to a copy of the request.
3. All original request forms and responses will remain a part of the data subject's record and shall be maintained as long as the underlying record is required to be maintained by the Commonwealth's record retention policies, or for six years, whichever is longer.
4. If the request involves confidential information maintained by more than one Center or by a covered and non-covered component of the same Center, the Center that received the request should forward a copy of the request to the Privacy Office, which will coordinate the processing of the request.

C. Email or Telephone Requests

Data subjects making a request for individual rights by telephone or e-mail should be sent a copy of the necessary form, if applicable.

D. Timely Review

Centers shall respond to all requests within thirty (30) days of receipt of the written request. For request for access to information that is not maintained or accessible on-site, the response shall be no later than sixty (60) days. One thirty-day extension is allowed provided that the data subject is notified of the reason for the delay and the date the Department will comply with the request.

E. Fees

Centers may charge twenty cents ($.20) a page for photocopies, or the actual cost incurred for records not susceptible to ordinary means of reproduction and the cost of postage. If a summary of the confidential information was agreed to by the data subject, the agreed upon cost of the summary may be included. MDPH Hospitals shall follow the fee schedules established for the hospitals.

F. Covered and Non-Covered Component Response Forms

All forms are specific to covered and non-covered component:

- Covered Components (labeled with the prefix CC): reflects the ability of data subjects to file complaints with MDPH's Privacy Office or to the Secretary of Health and Human Services.
- Non-Covered Components (labeled with the prefix NCC): reflects that data subjects may file a complaint only with MDPH's Privacy Office.

G. Documentation

Centers must document the designations and procedures required under this procedure. This documentation must be maintained for a minimum of six years, or as required by the Massachusetts Records Conservation Board.[45]

[45] Information related to the Massachusetts Records Conservation Board is available at http://www.state.ma.us/sec/arc/arcrcb/rcbidx.htm.

Authority: M.G.L. c.66A, §§ 2(i) and (j);
45 C.F.R. §§ 164.522, 164.524, and 164.526.

Forms: Request for Access to Confidential Information
Request for Amendment of Confidential Information
Request for Alternative Means of Communication
Request for Restrictions on Use and Disclosures of Confidential Information
http://healthnet/privsec/forms.htm

Procedure Title:	Accounting of Disclosures		
Procedure Number:	12	**Version #**	2.0
Effective Date:	May 3, 2004		

Content

I. Purpose and Scope

This procedure describes the procedures Centers should follow in response to requests by data subjects for an accounting of the disclosures of their confidential information.

This procedure applies to both covered and non-covered components of the Department and all Department workforce members. As described below, there are specific requirements that relate only to covered components and their workforce members.

II. General Requirements

Generally, each data subject has a right to request and receive a descriptive list, known as an accounting, of all the disclosures of his or her confidential information made by the Department.[46] However, Centers are not required to account for disclosures:

- To the data subject or the data subject's personal representative;
- Pursuant to an authorization;
- For treatment, payment and operations;

[46] The accounting requirements apply only to the release of confidential information that is defined as a disclosure under Procedure # 3: Use and Disclosure of Confidential Information. Since unrestricted identifiable vital record information disclosed by the Registry of Vital Records and Statistics is not considered confidential information, no accounting is required for such disclosures.

- For national security or intelligence purposes;
- To correctional institutions or law enforcement officials as permitted under law;
- Incident to a disclosure that is otherwise permitted or required under Procedure # 3: Use and Disclosure of Confidential Information;
- As part of a limited data set as described in Procedure #7: Requirements for De-Identification, Limited Data Sets and Aggregate Data;
- Limited to information that is de-identified in accordance with consistent with Procedure #7;
- In response to a public records request that have been redacted in accordance with Procedure # 8: Public Records Release Standards for MDPH Documents Containing Medical Information; and
- Made prior to April 14, 2003.

Questions about whether a particular disclosure must be included in an accounting of disclosures should be referred to the Center or Bureau privacy liaison first, and then the Privacy Office.

III. Accounting Requirements for Covered Components

Covered components must also account to the data subject for disclosures made:

- By business associates as described in Procedure # CC-2: Business Associate Agreements; and
- To another covered or non-covered component of the Department as described in Procedure # 3.

IV. Implementation: Center Responsibilities

DPH Centers shall develop procedures for maintaining the record of disclosures necessary to produce an accounting. This record may be combined with the Record of Disclosure required in Procedure # 3. This requirement can be met by:

- Maintaining a paper or electronic disclosure log, which tracks each disclosure required in an accounting as they are made; or
- Compiling the required accounting upon receipt of a data subject's request utilizing existing Center records.

A. Requests in Writing

A data subject's request for an accounting must be made in writing, and if possible, using the form *Request for Access to Confidential Information*.[47] Any request for an accounting of disclosures shall include the following:

1. The name of the data subject making the request;

[47] Versions of the form specific to covered and non-covered components are available at http://healtnet/privsec/forms.htm

2. Identification of programs or records for which the data subject is seeking an accounting; and
3. The time period for which the accounting is based, not to exceed six years prior to the date of the request, or for disclosures made prior to April 14, 2003.

B. Review of Requests

Upon receipt of a request for an accounting of disclosures, DPH Centers shall review the request and prepare the accounting. If the accounting is for confidential information from more than one Center, or for covered and non-covered components within the same Center, the Center receiving the request should contact the Privacy Office, which will coordinate the response. The Privacy Office shall also process requests for a Department-wide accounting.

C. Temporary Suspension of Accounting

In limited circumstances there may be a temporary suspension of a data subject's right to receive an accounting due to a request from a health oversight agency or a law enforcement official. All requests to suspend an accounting of a data subject's confidential information should be referred directly to the Office of General Counsel or the Privacy Office. If the request is deemed valid, the accounting will temporarily be suspended.

1. Requests in Writing

If the request for the temporary suspension of the individual's right to receive an accounting is in writing and includes a statement of the reasons that an accounting would likely impede the requestor's activities and includes the time period for such a suspension, the Department will grant the request for the suspension. The time period of the suspension shall not exceed one year from the date that the requestor's commenced an investigation of the individual.

2. Oral Requests

If the request is made orally, Centers shall attempt to get it in writing. If this is not possible, the oral request should be documented by the Center, listing the verified identity[48] of the individual making the request for suspension, and the reasons for the request. If the request is deemed valid, the data subject's right to an accounting will be suspended for no more than thirty (30) days, unless a written request submitted during that time frame specifies the time frame required for the suspension.

D. Content of Accounting: General Requirements

The accounting provided for each data subject's request must include for each disclosure made during the time period requested:

1. The date of the disclosure;

[48] The requestor's identity should be verified in accordance with Procedure # 9: Verification of Individuals or Entities Requesting Confidential Information.

2. The name of the entity or person who received the confidential information and, if known, the address of such entity or person;
3. A brief description of the confidential information disclosed; and
4. A brief statement of the purpose of the disclosure that reasonably informs the data subject of the basis for the disclosure. In lieu of such a statement, a copy of the written request for the disclosure made be provided.

E. Accounting for Multiple Disclosures

If during the requested period for accounting, multiple disclosures have been made to the same entity or person for a single purpose, the accounting does not need to list each disclosure in detail. Rather, the accounting may list:

- The first and last dates of the series of disclosures,
- The frequency or number of disclosures, and
- Elements 2, 3, and 4 listed in section IV.D.

F. Accounting for Research

Unless the information disclosed is de-identified or constitutes a limited data set, Centers must account for disclosures made for research purposes. The content of the accounting for research depends on the number of participants in the research study.

1. 50 or fewer Participants
   Each Center or Bureau that discloses confidential information for a research study involving 50 or fewer participants must provide, an accounting of each disclosure in accordance with the requirements of section IV.D and section IV.E.

2. 50 or more Participants
   If confidential information about the individual requesting the accounting may have been disclosed as part of a research study involving more than 50 participants, the following information must be included in the accounting:
   - The name of the protocol or research activity;
   - A description, in plain language, of the protocol or activity, including its purpose and the criteria for selecting particular records;
   - A brief description of the type of confidential information disclosed;
   - The date or time period during which the disclosures occurred or may have occurred, including the last disclosure date;
   - The name, address and phone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
   - A statement that the confidential information may or may not have been disclosed for a particular protocol or other research activity.

G. Center Designations

All Centers shall designate one or more individuals to be responsible for maintaining the log of disclosures required by Procedure # 3, as well as responding to requests for an accounting of disclosures. Centers may choose to do this at the Bureau or program level.

H. Documentation

Centers must maintain the following documentation for a minimum of six (6) years, or longer if required by the Commonwealth's Records Conservation Board:[49]

1. A copy of the current and previous versions of the procedures necessary to produce an accounting;
2. A list of the designated individual(s) responsible for implementing the procedures for accounting; and
3. A record of all requests for an accounting and all responses to these requests.

The documentation must be made accessible to the Privacy Office upon request.

I. Fees

The first request for an accounting within a 12 month period is free. The following is the fee structure for subsequent requests:

1 year of accounting $2.00	4 years of accounting $5.00
2 years of accounting $3.00	5 years of accounting $6.00
3 years of accounting $4.00	6 years of accounting $7.00

Authority: M.G.L. c. 66A, §§ 2(f), (g) and (i)
45 C.F.R. § 164.528
Forms: Request for Accounting of Disclosures

[49] Information related to the Massachusetts Records Conservation Board is available at http://www.state.ma.us/sec/arc/arcrcb/rcbidx.htm.

Procedure Title:	Complaints Regarding the Use and Disclosure of Confidential Information		
Procedure Number:	13	**Version #**	2.0
Effective Date:	May 3, 2004		

Content

I. Purpose and Scope

This procedure describes a data subject's right to file a complaint if he or she believes his or her rights under the Department's Confidentiality Policy and Procedures have been violated.

This procedure applies to both covered and non-covered components of the Department. As described below, there are a certain requirements that apply only to covered components.

II. Process for Filing a Complaint[50]

A. General Requirements

1. All complaints must be in writing when feasible, and sent to:

Massachusetts Department of Public Health
Privacy Office
250 Washington St., 2nd Floor
Boston, MA 02108

2. All written complaints should be made using the Department's privacy complaint form.[51] If a data subject or the subject's representative calls to file a complaint, he or she should be sent a copy of the Department's privacy complaint form.

[50] Complaints relating to DPH Hospitals or the State Office of Pharmacy Services, and all questions regarding their respective complaint procedures must be submitted to their respective privacy offices.

[51] The Privacy Complaint forms for both covered and non-covered components are available at: http://heathnet/privsec/forms.htm.

3. All complaints must be filed within one hundred eighty (180) days of when the individual knew or should have known of the alleged violation.
4. Questions about filing complaints should be referred to (617) 624-6083.

B. Requirements for Covered Components

In addition to registering complaints with MDPH, individuals may register a complaint with the U.S. Department of Health and Human Services at:

Office for Civil Rights
US Dept. of Health and Human Services
Government Center
J.F. Kennedy Federal Building-Room 1875
Boston, MA 02203
Voice Phone (617) 565-1340
Fax (617) 565-3809/TDD (617) 565-1343

III. Investigation of Complaints

Upon receipt of a complaint, the Privacy Officer, in consultation with the Director of the Center involved in the complaint, shall complete the following:

A. Consult with the Center Director or Hospital Director, if necessary, and determine whether the complaint should be investigated by the Center's privacy liaison or Hospital privacy contact, or the Privacy Officer, based on the nature of the alleged facts. In most instances, the complaint will be investigated by the Center or the Hospital;

B. Interview the individual who filed the complaint (the complainant) to ensure a full understanding of the alleged violation;

C. Meet with staff, as applicable, who have knowledge of the complaint or issues associated with it;

D. Complete a draft response containing proposed findings, and forward it to the appropriate Center director, or designee, for review and approval;

E. Send the final response to the complainant, and maintain a copy in the Privacy Office's files for six (6) years or longer, if required by the Records Conservation Board.[52]

F. Maintain a log that documents all complaints received, the disposition, and the date of disposition.

Authority: M.G.L. c. 66A, § 2
45 C.F.R. § 164.530(d)

Forms: CC and NCC Privacy Complaint Forms

[52] Information related to the Massachusetts Records Conservation Board is available at http://www.state.ma.us/sec/arc/arcrcb/rcbidx.htm.

Massachusetts Department of Public Health
Confidentiality Procedures

Procedure Title:	Notice of Privacy Practices		
Policy Number:	CC-1	**Version #**	2.0
Effective Date:	May 3, 2005		

Content

I. Purpose and Scope

This procedure describes the requirements related to the provision of a Notice of Privacy Practices (Notice) by the Department's covered components. Specific requirements related to providing and distributing the Notice depend on the type of covered component as described in section V. All workforce members in the Department's covered components must comply with this procedure.

II. General Requirements

Under the Privacy Rule, a data subject has a right to adequate notice of:

- The uses and disclosures of his or her confidential health information that may be made by or on behalf of the covered component; and,
- The data subject's rights and the covered component's legal duties with respect to the data subject's confidential health information.

There is no model Notice for the Department. Rather, each component must create its own Notice incorporating the requirements listed below.

III. Required Content

The Notice must be written in plain language and include the following heading:

"THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."

A. Uses and Disclosures

The Notice must include descriptions of the elements listed in the following categories, written in sufficient detail to describe the uses and disclosures of confidential information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to confidential information.

1. A description of the types of uses and disclosures that the covered component is permitted to make for purposes of treatment, payment, and health care operations, including at least one example for each;
2. A description of each of the other purposes for which the covered component is permitted or required to use or disclose confidential health information without a data subject's authorization;
3. A description of any restrictions on the use and disclosure of confidential information limited by any state or federal laws, which are not preempted by HIPAA and which are more stringent than HIPAA;
4. A statement that other uses or disclosures will be made only with the data subject's written authorization, and that an individual's authorization may be revoked as provided for in the Rule;
5. A separate statement describing if a provider intends to contact the data subject for appointment reminders, treatment alternatives or other health related benefits; and
6. Although not mandated, a description that confidential health information may be disclosed to business associates is recommended.

B. Rights of the Data Subject

1. A statement of the data subject's rights with respect to confidential health information and a description of how the data subject may exercise these rights, including:
    - The right to restrictions on certain uses/disclosures of confidential health information, including a statement that the covered component is not required to agree to a requested restriction;
    - The right to receive confidential communications of confidential health information;
    - The right to inspect and copy confidential health information;
    - The right to amend confidential health information;
    - The right to receive an accounting of disclosures of confidential health information; and,
    - The right to receive a paper copy of the Notice of Privacy Practices.

2. A statement that data subjects may complain to the covered component and to the Secretary of U.S. Department of Health and Human Services about privacy violations, including a brief description of how a complaint may be filed and a statement that the data subject will not be retaliated against for filing a compliant; and
3. The name or title, and the telephone number of the person or office for further information related to the covered component's complaint process.

C. Obligations of the Covered Component

1. A statement that the covered component is required by law to maintain the privacy of confidential health information and to provide data subjects with notice of its legal duties and privacy practices with respect to protected health information;
2. A statement that the covered component is required to abide by the terms of the Notice currently in effect; and
3. A statement that the covered component reserves the right to change the terms of the Notice and to make the new Notice provisions effective for all confidential health information that it maintains and a description of how the covered component will provide data subjects with a revised Notice.

D. Effective Date

The Notice must include the effective date, which may not be earlier than the date on which it is first printed or published.

IV. Revisions

The covered component must promptly revise and distribute the Notice when there is a material change to its uses or disclosures of confidential information, the data subject's rights, the covered components legal duties, or other privacy practices described in the Notice. Except when required by law, a material change to any term may not be implemented prior to the effective date of the Notice reflecting the change.

V. Provision and Distribution of the Notice

A. Covered component health plans need only provide their Notice to the data subject who is the named insured. The Notice must be distributed as follows:

1. No later than April 14, 2003, for data subjects covered by the plan at that time;
2. For new enrollees, at the time of enrollment;
3. Within 60 days of a material revision to the Notice, to data subjects then covered by the plan; and
4. At least once every 3 years, data subjects covered by the plan must be notified of the availability of the Notice and how to obtain the Notice.

B. Covered component direct health care providers are required to affirmatively provide the Notice only when there is a direct treatment relationship with the data subject. The Notice must be distributed as follows:

1. No later than the date of the first service delivery, after April 14, 2003, or as soon as reasonably practicable in an emergency situation;
2. The covered component provider shall make a good faith effort to obtain a written acknowledgement of receipt of the Notice from the data subject or document why acknowledgment was not obtained;
3. Post the current Notice in effect, and make copies available, at the service delivery site;
4. Post the current Notice in effect on the covered component's web site; and
5. Upon revision, make the revised Notice available upon request and prominently post the Notice at the site of service delivery.

C. Covered component indirect health care providers such as clinical laboratories, are only required to distribute a Notice upon request.

D. Distribution by Business Associates[53]

1. A covered health care component can make arrangements with a business associate (BA) to distribute its Notice. However, the covered component remains responsible for the Notice.
2. If a MDPH covered component arranges for its BA to distribute the Notice, this must be explicitly stated in the BA agreement, along with a requirement that the BA demonstrate full compliance with this obligation. If the BA is a provider on the covered component's behalf, it will need to make a good faith effort to obtain an acknowledgement of receipt of the Notice and maintain or provide to the covered component the acknowledgement documentation.

VI. Documentation Requirements

The covered component must retain the following documentation for six (6) years, or longer if required by the Commonwealth's Records Conservation Board[54]:

- Copies of all Notices issued, including those no longer in effect; and
- Copies of written acknowledgments or the documentation of good faith efforts to obtain acknowledgment.

Authority: 45 C.F.R. § 164.520

[53] Procedure # CC-2: Business Associate Agreements describes the contractual requirements between programs and their BAs in detail.

[54] Information related to the Massachusetts Records Conservation Board is available at http://www.state.ma.us/sec/arc/arcrcb/rcbidx.htm.

Massachusetts Department of Public Health
Confidentiality Procedures

Procedure Title:	Business Associate Agreements		
Procedure Number:	CC-2	**Version #**	2.0
Effective Date:	May 3, 2004		

Content

I. Purpose and Scope

This procedure provides instructions to all covered components regarding the necessity for and the required content of agreements with a business associate (BA). It pertains to the BAs receipt, use and development of confidential information from or on behalf of the MDPH covered component.

Programs that are not covered components are not required to enter into business associate agreements. However, it is recommended where there is sharing of confidential information with a contract vendor, that language covering the use, disclosure and security of such information be included when a contract is entered as described at http://healthnet/privsec/cagreements.htm.

II. General Requirements

The covered component may disclose confidential information to a BA, or allow a BA to create or receive confidential information on the covered component's behalf, if the covered component obtains adequate assurance that the BA will appropriately safeguard the confidential information. Such assurances shall be included in the underlying contract, an amendment to the underlying contract, or a separate Business Associate Agreement.

A. Each covered component should evaluate every contract it maintains where there is access to confidential health information, utilizing the Department's BA decision-tree.

B. Once a BA is identified, the covered component should work with the Office of General Counsel to adapt the Department's model business associate agreement for the particular BA relationship.

C. Each BA agreement, along with the underlying contract, should be maintained by the covered component for six (6) years, or longer if required by the Commonwealth's Records Conservation Board.[55]

III. Exceptions to the BAA Requirements

The BAA requirements do not apply to:

A. Disclosures by a covered entity to a health care provider for treatment of an individual;
B. Uses or disclosures made to another governmental agency for purposes of public health eligibility or enrollment determinations where such agency is authorized by law to make these determinations;
C. Contracts with persons or organizations whose functions do not involve the use of confidential information; or
D. The disclosure of confidential information to a researcher for research purposes either with an authorization, pursuant to a waiver, or as a limited data set.

III. Required Content

The agreement between the covered component and the BA must include language that provides that the business associate will:

A. Not use or further disclose the information other than as permitted or required by the contract or as required by law;
B. Use appropriate safeguards to prevent unauthorized use or disclosure of the information;
C. Report unauthorized uses or disclosures to the covered component;
D. Ensure that any agents, including a subcontractor, agree to the same restrictions and conditions that apply to the BA with respect to the confidential information;
E. Make confidential information available for access by the data subject or his/her personal representative within time frames established in the agreement;
F. Make confidential information available for amendment, and incorporate any approved amendments to confidential information, within time frames established in the agreement;
G. Make available the information required to provide a full accounting of disclosures, except for disclosures to the data subject, to his/her personal representative, or
H. Make its internal practices, books, and records relating to the use and disclosure of individually identifiable health information received from, or created by or on behalf of the organization, available to the U.S. Secretary of Health and Human Services for purposes of determining the covered component's compliance with HIPAA;

[55] Information related to the Massachusetts Records Conservation Board is available at http://www.state.ma.us/sec/arc/arcrcb/rcbidx.htm.

I. Return or destroy all confidential information received from, or created by or on behalf of the covered component at termination of the contract, if feasible. If such return or destruction is not feasible and any confidential information is retained, extend the full protections in the BA agreement as long as the confidential information is maintained and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

J. Be subject to termination of the agreement upon the BA's violation of a material term of the agreement.

IV. BA Agreements When Both Entities are Governmental Agencies

A. The covered component may comply with this procedure by entering into a Memorandum of Understanding (MOU) or Interagency Service Agreement (ISA) that contains terms that accomplishes the BA agreement objectives.

B. The covered component may comply with this procedure, *without* entering into an agreement, if other law (including regulations adopted by MDPH or the governmental agency that is the BA) contains requirements applicable to the BA that accomplish the objectives of a BA agreement.

C. The covered component may omit a termination procedure from the agreement if it is inconsistent with the statutory obligations of the covered component of the agency that is the BA.

V. BA Oversight Responsibility

There is no affirmative responsibility imposed by HIPAA to monitor the BA. However, if a covered component knows of a pattern or practice of the BA that amounts to a material violation of the BA agreement, the entity must attempt to mitigate the breach or end the violation. If the attempted mitigation is unsuccessful, the covered component shall terminate the agreement if feasible. If termination is not feasible, the covered component must report the problem to the Office of the U.S. Secretary of Health and Human Services.

Authority: 45 C.F.R. §§ 164.502(e)(1)(ii); 164.504(e)(2) and (3); 164.532(e)

Forms: Business Associate Agreement Model Forms
Business Associate Decision Tree

Procedure Title:	Designated Record Sets		
Procedure Number:	CC-3	**Version #**	2.0
Effective Date:	May 3, 2004		

Content

I. Purpose and Scope

This procedure defines the Designated Record Set (DRS) for covered components that are health care providers and health plans. The procedure also provides a checklist for covered components to use when determining which part of their confidential health information constitutes the Designated Record Set (DRS). All workforce members in the Department's covered components must comply with this procedure.

Unless otherwise limited, HIPAA requires that a covered component provide an individual, upon request, access to certain health information that constitutes a designated record set, as defined below. State law requirements under FIPA may require broader access to records than the HIPAA requirements. A covered component is required to comply with both statutes.

II. Definitions

A. DRS for Health Care Providers

A group of "records"[56] maintained by the provider or for the provider that includes:

1. The medical records and billing records about data subjects maintained by the provider or by a third party for the provider; or
2. Used, in whole or in part, by the provider, or by a third party for the provider, to make decisions about data subjects.

B. DRS for Health Plans

A group of "records" maintained by the plan or for the plan that includes:

1. The enrollment, payment, claims adjudication, and case or medical management record systems maintained by the plan, or maintained by a third party for the plan; or

[56] A record is any item, collection, or grouping of information that includes confidential health information and is maintained, collected, used, or disseminated by or for a covered component.

2. Used, in whole or in part, by the plan, or by a third party for the plan, to make decisions about data subjects.

III. DRS Checklist

A. Workforce members should follow the steps in this checklist, which will enable the covered component to identify its DRS.

1. Identify the "storage sites" where confidential health information is stored:
- Include both paper and electronic systems;
- Include network and desktop systems;
- Include current files and archived files;[57]
- Include all sites; and
- Include all record systems in the possession of business associates and other agents.

2. Identify the following elements of the records that are included in the covered component's applicable DRS as defined in section II.

a. Health Care Providers

For each confidential health information "storage site" identified in section III.A.1, identify those that contain in whole or in part:

- Medical record(s) as defined by the covered component; and
- Billing record(s), including any records that might be developed by contracted vendors, Medicare maximization projects, etc.

b. Health Plans

For each confidential health information "storage site" identified in section III.A.1, identify those that contain in whole or in part:

- Enrollment record(s);
- Payment record(s);
- Claim adjudication record(s); and
- Case or medical management record(s).

3. Identify any additional records for each storage site which are used to make decisions about the data subject that are not included in section III.A.2.

a. Records which are used in making "decisions" about a data subject. For example, records regarding eligibility for a service, need for intervention,

[57] The DRS must go back six years. The time begins "running" as of April 14, 2003. For requests received on or after that date, it is likely the elements of the DRS are not archived. Prospectively, the location of records that are archived more frequently than every six years must be noted so they can be accessed if there is a request for the DRS that reaches back the full six years.

outcome of an appeal, need for medical supervision, or appropriateness for release. *These records are included in a DRS.*

b. Records not used to make decisions about a data subject. For example, records used for such things as tracking utilization, budget reporting, program assessment, "bed check" records, attendance reports, or billing back-up. *These records are not included in a DRS.*

4. Sort the records identified in subsections III.A.2 and 3(a), eliminating any duplicate records or redundancies. For example, if all of the information in one record is included in one or more other records, the first record can be eliminated as long as the other record or records remain as part of the DRS.

5. Document your DRS as containing all records remaining after step 4.

6. Determine if any part of the DRS meets any of the access exceptions:
a. Psychotherapy notes;
b. Information compiled in reasonable anticipation of, or for use in a civil, criminal, or administrative action or proceeding; and
c. Confidential health information maintained by the covered component that is:
- Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. § 263(a) to the extent the provision of access to the individual would be prohibited by law; or
- Exempt from the Clinical Laboratory Improvements Amendments of 1988, pursuant to 42 C.F.R. § 493.3(a)(2).

7. Create a business process to provide the data subject with access to his or her DRS.
a. Determine the process for setting apart records or parts of records, which are excepted from the access requirements.
b. If parts of the DRS are maintained at various sites, determine the most efficient manner of collecting them in one location if access request is made.
c. Determine the preferred means of handling access requests made directly to a business associate. For example, should all requests be forwarded to and handled at a central location? Should the business associate be required to have a process for providing access to the records maintained by the business associate? If so, what reporting mechanism is needed to provide a record of those requests and the materials provided?

8. If the request for access is limited to a DRS, then the workforce member is only required to provide the DRS. If the data subject requests information outside of the DRS, under state law this should also be provided to the data

subject unless there are limits on such access as described to Procedure # 11.

9. Create a business process to update the DRS when new confidential health information "storage sites" are created or existing ones are modified or deleted.

IV. Documentation

A covered component must document and retain the following for six (6) years, or longer if required by the Commonwealth's Records Conservation Board:[58]

- The designated record sets that are subject to access by data subjects; and
- The titles of persons or offices responsible for receiving and processing requests for access by data subjects.

Authority: 45 C.F.R. §§ 164.524; 164.530

[58] Information related to the Massachusetts Records Conservation Board is available at http://www.state.ma.us/sec/arc/arcrcb/rcbidx.htm.

Referenced Statutes/Regulations for Confidentiality Policy and Procedures

Massachusetts

M.G.L. c. 4, § 7(26): Public Records Law:

M.G.L. c. 66A: Fair Information Practices Act

M.G.L. c. 70F: HLTV-III test; confidentiality; informed consent

M.G.L. c. 111, § 24A: Reduction of morbidity and mortality; establishment of program; information and reports

M.G.L. c. 111, § 24B: Birth information; statistical purposes

M.G.L. c. 111, § 67E: Children born with congenital anomaly, birth defect, birth injury or mental retardation; reports

M.G.L. c. 111, § 202: Fetal deaths; reports; confidentiality; disposition of remains; violations; forms

Mass Executive Order 412: To Protect The Privacy Of Personal Information

Federal

42 C.F.R. Part 2: Confidentiality of Alcohol and Drug Abuse Patient Records

45 C.F.R. Part 46: Protection of Human Subjects (The Common Rule)

45 C.F.R. Parts 160 and 164: HIPAA Privacy Rule

45 C.F.R.§ 493.123: Laboratory Requirements - Standard: Confidentiality of Patient Information.